ION D. ION
A.P. GHIOCA
N.I. NEDIȚĂ

ALGEBRĂ

XII

MINISTERUL EDUCAȚIEI ȘI ÎNVĂȚĂMÎNTULUI

ION D. ION

A. P. GHIOCA

N. I. NEDIȚĂ

Matematică

XII

Algebră

Manual pentru clasa a XII-a



Editura Didactică și Pedagogică, București – 1989

§ 1. NUMERE

Peste tot în acest manual vom nota cu **N** mulţimea numerelor naturale,

$$\mathbf{N} = \{0, 1, 2, \ldots, n, \ldots\}.$$

Referitor la adunarea şi înmulţirea numerelor naturale acceptăm proprietăţile :

1) $(x + y) + z = x + (y + z)$,

2) $0 + x = x + 0 = x$,

3) $x + y = y + x$,

4) $(xy)z = x(yz)$,

5) $1 \cdot x = x \cdot 1 = x$,

6) $x(y + z) = xy + xz$,

7) $xy = yx$

oricare ar fi $x, y, z \in \mathbf{N}$.

De asemenea, vom nota cu **Z**, mulţimea numerelor întregi,

$$\mathbf{Z} = \{\ldots, -n, \ldots, -2, -1, 0, 1, 2, \ldots, n, \ldots\}.$$

Acceptăm ca adevărate pentru adunarea şi înmulţirea numerelor întregi proprietăţile 1) — 7) precum şi proprietatea :

8) $x + (-x) = (-x) + x = 0, \quad \forall x \in \mathbf{Z}$.

Vom nota cu **Q** mulţimea numerelor raţionale, $\mathbf{Q} = \{a/b \mid a, \ b \in \mathbf{Z}, \ b \neq 0\}$. Pentru $x \in \mathbf{Q}$, $x \neq 0$, $x = a/b$, notăm cu x^{-1} numărul raţional b/a. Avem :

9) $xx^{-1} = x^{-1}x = 1$,

oricare ar fi $x \in \mathbf{Q}$, $x \neq 0$.

Cu **R** va fi notată mulţimea numerelor reale, iar cu **C** mulţimea numerelor complexe, $\mathbf{C} = \{a + ib \mid a, \ b \in \mathbf{R}\}$. Pentru adunarea şi înmulţirea numerelor reale (complexe) acceptăm ca adevărate proprietăţile 1) — 9).

Avem :

$$\mathbf{N} \subset \mathbf{Z} \subset \mathbf{Q} \subset \mathbf{R} \subset \mathbf{C}.$$

Literele folosite mai sus pentru notarea mulţimilor de numere menţionate apar în textul manualului culese aldin (gras). Pentru scrierea lor cu

mîna (pe hîrtie sau la tablă...) la literele de tipar uzuale se adaugă o linie suplimentară. Aceste convenţii de notaţii sînt consacrate în literatura matematică actuală.

Se ştie că $\sqrt{2}$ *nu este număr raţional.* Să reamintim demonstraţia. Dacă $\sqrt{2} \in \mathbf{Q}$, atunci $\sqrt{2} = a/b$, cu $a, b \in \mathbf{Z}$, $b \neq 0$. Putem presupune că fracţia a/b este ireductibilă, adică a şi b nu admit nici un divizor comun $c \in \mathbf{Z}$ astfel încît $|c| > 1$. Cum $a^2 = 2b^2$ rezultă că a^2 este par, deci a este par, de unde $a = 2a_1$, cu $a_1 \in \mathbf{Z}$. Avem $4a_1^2 = 2b^2$, deci $2a_1^2 = b^2$. Rezultă că şi b este par, deci a şi b admit ca divizor comun pe 2. Contradicţie.

1.1. *Definiţie.* **Spunem că un număr întreg d diferit de 0 şi 1 este *liber de pătrate* dacă nu se divide prin pătratul nici unui număr prim.**

Astfel numerele 6, 2, -15, -1, -3 sînt libere de pătrate. Numerele 108 şi -40 nu sînt libere de pătrate căci $108 = 3^3 \cdot 2^2$, $-40 = (-5) \cdot 2^3$.

Dacă $d \geqslant 0$ atunci prin $\sqrt{d}$ notăm radicalul aritmetic al lui d, adică unicul număr real $\alpha \geqslant 0$ astfel încît $\alpha^2 = d$. Dacă $d < 0$, atunci $\sqrt{d} = i\sqrt{-d}$, unde $i^2 = -1$. Astfel $\sqrt{-3} = i\sqrt{3}$.

1.2. Teoremă. **Dacă d este un număr întreg liber de pătrate, atunci $\sqrt{d} \notin \mathbf{Q}$.**

Demonstraţie. Dacă $d < 0$, atunci $\sqrt{d}$ este număr complex şi deci $\sqrt{d} \notin \mathbf{Q}$. Rămîne să considerăm cazul $d > 1$. Dacă $\sqrt{d} \in \mathbf{Q}$ atunci $\sqrt{d} = a/b$, $a > 0$, $b > 0$ unde a/b este o fracţie ireductibilă. Avem $db^2 = a^2$ şi dacă $a = 1$, atunci $b^2d = 1$, deci $d = 1$. Contradicţie. Deci $a > 1$ şi atunci a admite un divizor prim p. Aşadar $a = pc$, cu $c \in \mathbf{Z}$, de unde $b^2d = p^2c^2$. Cum fracţia a/b este ireductibilă, p nu divide pe b, deci din egalitatea $b^2d = p^2c$ rezultă că p^2 divide pe d. Contradicţie.

Numerele de forma $a + b\sqrt{d}$, cu $a, b \in \mathbf{Q}$ şi d întreg liber de pătrate se numesc *numere pătratice*. Astfel :

$$1 + \sqrt{2},\ \frac{-1 + \sqrt{-3}}{2},\quad \frac{-1 + i\sqrt{3}}{2},\ 4 + 3\sqrt{5},\ 2 - 3i$$

sînt numere pătratice, unde $i^2 = -1$.

Dacă $a + b\sqrt{d}$ şi $a' + b'\sqrt{d}$ sînt două numere pătratice, atunci :

$$a + b\sqrt{d} = a' + b'\sqrt{d} \Leftrightarrow a = a' \text{ şi } b = b'.$$

În adevăr, dacă $a + b\sqrt{d} = a' + b'\sqrt{d}$ şi $b \neq b'$ atunci

$$\sqrt{d} = \frac{a - a'}{b - b'} \in \mathbf{Q}.$$

Contradicţie. Deci $b = b'$ şi atunci $a = a'$.

Dacă d este un întreg liber de pătrate, atunci notăm cu $\mathbf{Q}(\sqrt{d})$ mulţimea tuturor numerelor pătratice de forma $a + b\sqrt{d}$, cu $a, b \in \mathbf{Q}$ şi cu $\mathbf{Z}[\sqrt{d}]$ mulţimea tuturor numerelor pătratice de forma $a + b\sqrt{d}$ cu $a, b \in \mathbf{Z}$.

Aşadar :

$$\mathbf{Q}(\sqrt{d}) \overset{\text{def}}{=} \{a + b\sqrt{d} \mid a,\ b \in \mathbf{Q}\}$$

şi

$$\mathbf{Z}[\sqrt{d}] \overset{\text{def}}{=} \{a + b\sqrt{d} \mid a,\ b \in \mathbf{Z}\}.$$

Evident

$$\mathbf{Z} \subset \mathbf{Z}[\sqrt{d}] \subset \mathbf{Q}(\sqrt{d}) \subset \mathbf{C},$$

iar cînd $d > 0$, avem chiar $\mathbf{Q}(\sqrt{d}) \subset \mathbf{R}$.

Astfel :

$$\mathbf{Q}(\sqrt{2}) = \{a + b\sqrt{2} \mid a,\ b \in \mathbf{Q}\} \subset \mathbf{R}$$

şi

$$Z[\mathrm{i}] := \{a + b\mathrm{i} \mid a,\ b \in \mathbf{Z}\} \subset \mathbf{C}.$$

Dacă $z = a + b\sqrt{d}$ este un număr pătratic, atunci numărul pătratic $z^* = a - b\sqrt{d}$ se numeşte *conjugatul* lui z.

§ 2. MULŢIMI ŞI FUNCŢII (recapitulare)

Fie E o mulţime. Vom nota cu $\mathfrak{P}(E)$ mulţimea tuturor părţilor (submulţimilor) lui E. Dacă $X,\ Y \in \mathfrak{P}(E)$, atunci cu $X \cup Y$ şi $X \cap Y$ vom nota *reuniunea*, respectiv *intersecţia* lui X cu Y,

$$X \cup Y \overset{\text{def}}{=} \{x \in E \mid x \in X \text{ sau } x \in Y\}$$

respectiv

$$X \cap Y \overset{\text{def}}{=} \{x \in E \mid x \in X \text{ şi } x \in Y\}.$$

Amintim următoarele proprietăţi ale reuniunii şi intersecţiei :

1) $(X \cup Y) \cup Z = X \cup (Y \cup Z)$, $(X \cap Y) \cap Z = X \cap (Y \cap Z)$;

2) $\varnothing \cup X = X \cup \varnothing = X$, $E \cap X = X \cap E = X$;

3) $X \cup Y = Y \cup X$, $X \cap Y = Y \cap X$;

4) $X \cup (Y \cap Z) = (X \cup Y) \cap (X \cup Z)$, $X \cap (Y \cup Z) =$
$= (X \cap Y) \cup (X \cap Z)$

oricare ar fi $X,\ Y,\ Z \in \mathfrak{P}(E)$, unde $\varnothing$ este submulţimea *vidă* a lui E.

Fie E şi F două mulţimi. Pentru o funcţie $f : E \to F$ vom preciza uneori şi acţiunea lui f asupra elementelor $x \in E$ prin notaţia

$$f : E \to F,\ x \to f(x)$$

unde $f(x)$ este *imaginea* lui x prin f.

Fie E o mulţime. Vom nota cu $\mathcal{F}(E)$ mulţimea tuturor funcţiilor $f : E \to E$. Dacă $f, g \in \mathcal{F}(E)$, atunci funcţia

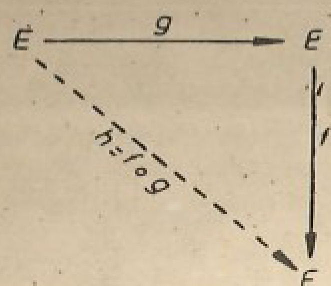


Fig. I.1.

$$h : E \to E, \ x \to h(x) \overset{\text{def}}{=} f(g(x))$$

se notează cu fog şi se numeşte *compusa* funcţiei f cu funcţia g (v. fig. I.1).

Funcţia $1_E : E \to E$, $1_E(x) = x$, $\forall x \in E$, se numeşte *aplicaţia identică* a mulţimii E.

2.1. Teoremă. Compunerea funcţiilor are proprietăţile:

1) $(fog)oh = fo(goh)$ $\qquad \forall f, g, h \in \mathcal{F}(E)$,

2) $1_E of = fo1_E = f$ $\qquad \forall f \in \mathcal{F}(E)$.

Demonstraţie. Pentru orice $x \in E$ avem:

$$((fog)oh)(x) = (fog)(h(x)) = f(g(h(x)))$$

şi

$$(fo(goh))(x) = f((goh)(x)) = f(g(h(x)))$$

de unde

$$(fog)oh = fo(goh).$$

De asemenea, pentru orice $x \in E$ avem:

$$(1_E of)(x) = 1_E(f(x)) = f(x) = f(1_E(x)) = (fo1_E)(x),$$

deci

$$1_E of = fo1_E = f.$$

O funcţie $f : E \to F$ se numeşte *injectivă* dacă $f(x_1) \neq f(x_2)$ oricare ar fi $x_1, x_2 \in E$, $x_1 \neq x_2$, ceea ce revine la:

$$f(x_1) = f(x_2) \Rightarrow x_1 = x_2.$$

Spunem că funcţia $f : E \to F$ este *surjectivă* dacă:

$$\forall y \in F, \ \exists x \in E \text{ astfel încît } y = f(x).$$

O funcţie $f : E \to F$ se numeşte *bijectivă* dacă este injectivă şi surjectivă.

2.2. Teoremă. Fie E o mulţime şi $f, g \in \mathcal{F}(E)$. Dacă f şi g sînt funcţii injective (surjective, bijective) atunci fog este funcţie injectivă (respectiv surjectivă, bijectivă).

Demonstraţie. Fie $h = fog$. Presupunem că f şi g sînt injective şi fie $x_1, x_2 \in E$ astfel încît $h(x_1) = h(x_2)$. Rezultă că $f(g(x_1)) = f(g(x_2))$. Cum f este funcţie injectivă rezultă că $g(x_1) = g(x_2)$, de unde $x_1 = x_2$ căci şi g este funcţie injectivă. Aşadar $h = fog$ este funcţie injectivă.

Presupunem că f şi g sînt funcţii surjective şi fie $z \in E$. Cum f şi g sînt funcţii surjective, există $y \in E$ astfel încît $z = f(y)$ şi există $x \in E$ astfel încît $y = g(x)$, de unde

$$z = f(y) = f(g(x)) = (f \circ g)(x) = h(x),$$

deci $h = f \circ g$ este funcţie surjectivă. Ultima afirmaţie este acum evidentă.

Dacă E şi F sînt două mulţimi, vom nota cu $E \setminus F$ mulţimea

$$E \setminus F = \{x \in E \mid x \notin F\}$$

numită *diferenţa* dintre E şi F (în această ordine). Cu $E \times F$ vom nota *produsul cartezian* al lui E cu F, adică mulţimea tuturor perechilor ordonate (x, y), cu $x \in E$ şi $y \in F$,

$$E \times F \overset{\text{def}}{=} \{(x, y) \mid x \in E, y \in F\}.$$

§ 3. MATRICE (recapitulare)

Notăm cu $M_2(\mathbf{R})$ mulţimea tuturor matricelor pătratice A de ordin 2 cu coeficienţi din $\mathbf{R}$,

$$A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}, \ a_{ij} \in \mathbf{R}.$$

Vom folosi şi scrierea mai condensată : $A = (a_{ij})$.

Dacă $A, B \in M_2(\mathbf{R})$, $A = (a_{ij})$, $B = (b_{ij})$, atunci *suma* $A + B$ a matricei A cu matricea B se defineşte prin :

$$A + B \overset{\text{def}}{=} \begin{pmatrix} a_{11} + b_{11} & a_{12} + b_{12} \\ a_{21} + b_{21} & a_{22} + b_{22} \end{pmatrix} \in M_2(\mathbf{R}).$$

De asemenea, *produsul* AB al matricei A cu matricea B se defineşte prin :

$$AB \overset{\text{def}}{=} \begin{pmatrix} a_{11}b_{11} + a_{12}b_{21} & a_{11}b_{12} + a_{12}b_{22} \\ a_{21}b_{11} + a_{22}b_{21} & a_{21}b_{12} + a_{22}b_{22} \end{pmatrix} \in M_2(\mathbf{R}).$$

Matricele 0, E şi $-A$ din $M_2(\mathbf{R})$,

$$0 = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \ E = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \ -A = \begin{pmatrix} -a_{11} & -a_{12} \\ -a_{21} & -a_{22} \end{pmatrix}$$

se numesc respectiv *matricea zero*, *matricea unitate*, *opusa matricei* A.

Avem următoarele proprietăţi ale adunării şi înmulţirii matricelor din $M_2(\mathbf{R})$:

1) $(A + B) + C = A + (B + C)$,

2) $0 + A = A + 0 = A$,

3) $A + (-A) = (-A) + A = 0$,

4) $A + B = B + A$,

5) $(AB)C = A(BC)$,

6) $EA = AE = A$,

7) $A(B + C) = AB + AC$; $(B + C)A = BA + CA$

oricare ar fi $A, B, C \in M_2(\mathbf{R})$. După cum se știe din clasa a XI-a, demonstrarea lor se face invocînd proprietăți similare ale operațiilor cu numere reale. Astfel :

$$A + (-A) = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} + \begin{pmatrix} -a_{11} & -a_{12} \\ -a_{21} & -a_{22} \end{pmatrix} =$$

$$= \begin{pmatrix} a_{11} + (-a_{11}) & a_{12} + (-a_{12}) \\ a_{21} + (-a_{21}) & a_{22} + (-a_{22}) \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} = 0$$

și analog, $(-A) + A = 0$.

Vom nota cu $M_2(\mathbf{Z})$, $M_2(\mathbf{Q})$, $M_2(\mathbf{C})$ mulțimea matricelor pătratice de ordin 2 cu coeficienți în $\mathbf{Z}$, $\mathbf{Q}$, $\mathbf{C}$, respectiv. În general, pentru $n > 1$, notăm cu $M_n(\mathbf{Z})$, $M_n(\mathbf{Q})$, ... mulțimea matricelor pătratice de ordin n cu coeficienți în $\mathbf{Z}$, $\mathbf{Q}$, ..., respectiv.

Dacă $A \in M_2(\mathbf{R})$, $A = (a_{ij})$, vom nota cu $\det(A)$ *determinantul* matricei A,

$$\det(A) = \begin{vmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{vmatrix} = a_{11}a_{22} - a_{21}a_{12} \in \mathbf{R}.$$

3.1. Teoremă. Oricare ar fi $A, B \in M_2(\mathbf{R})$, $A = (a_{ij})$, $B = (b_{ij})$, avem :

$$\det(AB) = \det(A)\det(B).$$

Demonstrație. Avem :

$$AB = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}\begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix} = \begin{pmatrix} a_{11}b_{11} + a_{12}b_{21} & a_{11}b_{12} + a_{12}b_{22} \\ a_{21}b_{11} + a_{22}b_{21} & a_{21}b_{12} + a_{22}b_{22} \end{pmatrix}.$$

Pe de altă parte, se observă că avem identitatea :

$$(a_{11}b_{11} + a_{12}b_{21})(a_{21}b_{12} + a_{22}b_{22}) - (a_{21}b_{11} + a_{22}b_{21})(a_{11}b_{12} + a_{12}b_{22}) =$$

$$= (a_{11}a_{22} - a_{21}a_{12})(b_{11}b_{22} - b_{21}b_{12}),$$

de unde

$$\det(AB) = \det(A)\det(B).$$

Exemplu

Dacă $A \in M_2(\mathbf{R})$, $A = \begin{pmatrix} 2 & 1 \\ 5 & 2 \end{pmatrix}$, atunci

$$\det(A^n) = (-1)^n \text{ oricare ar fi } n = 1, 2, \ldots .$$

În adevăr, $\det(A) = 2 \times 2 - 5 \times 1 = -1$ și deci afirmația este adevărată pentru $n = 1$. Presupunem că $n > 1$ și că $\det(A^{n-1}) = (-1)^{n-1}$. Atunci :

$$\det(A^n) = \det(A^{n-1} \cdot A) = \det(A^{n-1}) \det(A) = (-1)^{n-1} \cdot (-1) = (-1)^n.$$

§ 4. NUMERE RELATIV PRIME (recapitulare)

Fie a și b două numere întregi. Un număr $d \in \mathbf{Z}$, $d \geqslant 0$, se numește *cel mai mare divizor comun* (c.m.m.d.c.) al lui a și b dacă :

(1) $d \mid a$ și $d \mid b$;

(2) $c \mid a$ și $c \mid b \Rightarrow c \mid d$.

Dacă $d' \in \mathbf{Z}$, $d' \geqslant 0$, satisface, de asemenea, (1) și (2), atunci avem $d' \mid d$ și $d \mid d'$ de unde $d' = d$. Așadar, c.m.m.d.c. al numerelor a și b, în caz că există, este unic determinat. Pentru c.m.m.d.c. al lui a și b folosim notația $d = (a, b)$.

4.1. Teoremă. **Fie $a, b \in \mathbf{Z}$. Atunci c.m.m.d.c. al lui a și b există. Mai mult, dacă $d = (a, b)$ atunci există $h, k \in \mathbf{Z}$ astfel încît**

$$d = ah + bk.$$

Demonstrație. Dacă $a = b = 0$, atunci $d = 0$ și $0 = 0h + 0k$, unde h, k pot fi luați chiar arbitrar din $\mathbf{Z}$ în acest caz.

Presupunem că $a \neq 0$ sau $b \neq 0$. Fie $d = ah + bk$ cel mai mic număr strict pozitiv printre numerele de forma :

$$ax + by \qquad x, y \in \mathbf{Z}$$

(arătați că printre ele se găsesc numere strict pozitive !).

Dacă $c \mid a$ și $c \mid b$, atunci c divide și pe $ah + bk = d$, deci d satisface (2) din definiția c.m.m.d.c. Rămîne să mai arătăm că $d \mid a$ și $d \mid b$.

Dacă d nu divide pe a, există $q, r \in \mathbf{Z}$ astfel încît

$$a = dq + r, \qquad 0 < r < d.$$

Atunci

$0 < r = a - dq = a - (ah + bk)q = a(1 - hq) + b(-kq) < d$, ceea ce contrazice alegerea lui d. Rămîne adevărat că $d \mid a$. Analog se arată că $d \mid b$

Fie $a, b \in \mathbf{Z}$. Vom spune că a este *relativ prim* cu b dacă $(a, b) = 1$. Evident, a este relativ prim cu b dacă și numai dacă există $h, k \in \mathbf{Z}$ astfel încît $ah + bk = 1$.

4.2. Teoremă. **Fie $a, b, c \in \mathbf{Z}$. Avem :**

1) Dacă $(a, b) = 1$ și $(a, c) = 1 \Rightarrow (a, bc) = 1$;

2) Dacă $(a, b) = 1$ și $a \mid bc \Rightarrow a \mid c$;

3) Dacă $(a, b) = 1$, $a \mid c$ și $b \mid c \Rightarrow ab \mid c$.

Demonstrație. 1) Fie $h, k, u, v \in \mathbf{Z}$ astfel încît $1 = ah + bk$ și $1 = au + cv$. Atunci :

$1 = ah + bk(au + cv) = a(h + bku) + bc(kv)$, de unde $(a, bc) = 1$.

2) Fie $h, k \in \mathbf{Z}$ astfel încît $ah + bk = 1$. Atunci $c = a(hc) + bck$. Cum $a \mid a$ și $a \mid bc$ rezultă că a divide numărul $a(hc) + bc \cdot k = c$.

3) Fie $h, k \in \mathbf{Z}$ astfel încît $ah + bk = 1$. Atunci $c = ac \cdot h + bc \cdot k$. Cum $a \mid c$ și $b \mid c$ rezultă că $ab \mid ac$ și $ab \mid bc$, deci ab divide numărul $ac \cdot h + bc \cdot k = c$.

Exemple

1. Dacă $p > 0$ este un număr prim, atunci :

$$(a, p) = 1 \quad \forall a \in \mathbf{Z}, \quad 1 \leqslant a < p.$$

În adevăr, p fiind număr prim, singurii săi divizori pozitivi sînt 1 și p. Cum $1 \leqslant a < p$, p nu poate divide pe a. Rezultă că singurul divizor comun al lui a și p este 1 și atunci și c.m.m.d.c. al lui a și p este 1.

2. Pentru orice $n \in \mathbf{N}$, numărul $n^3 - n$ se divide prin 6. În adevăr, $n^3 - n = (n - 1)n(n + 1)$, deci $n^3 - n$ se divide prin 2 și 3. Cum $(2, 3) = 1$, rezultă că $n^3 - n$ se divide și prin $2 \times 3 = 6$.

3. Dacă $p > 0$, $q > 0$ sînt două numere prime distincte, atunci :

$$(p^m, q^n) = 1 \qquad \forall m, n \in \mathbf{N}.$$

În adevăr, să presupunem că $p < q$. Atunci conform cu rezultatul de la Ex. 1 avem $(p, q) = 1$. Presupunem că $(p, q^{n-1}) = 1$. Folosind Teorema 4.2, pct. 1) din $(p, q) = 1$ și $(p, q^{n-1}) = 1$ rezultă $(p, q^n) = 1$. Acum se fixează n și se demonstrează prin inducție asupra lui m că $(p^m, q^n) = 1$.

Exerciții rezolvate

R — 1 Fie E o mulțime și $f, g \in \mathcal{F}(E)$. Avem :

1) Dacă $f \circ g$ este funcție injectivă (surjectivă) atunci g este funcție injectivă (resp. f este funcție surjectivă) ;

2) Dacă $f \circ g = 1_E$, atunci g este funcție injectivă și f este funcție surjectivă ;

3) Dacă $f \circ g = g \circ f = 1_E$, atunci f și g sînt funcții bijective.

Soluție. 1) Presupunem că $f \circ g$ este funcție injectivă și fie $x_1, x_2 \in E$ astfel încît $g(x_1) = g(x_2)$. Atunci

$$(f \circ g)(x_1) = f(g(x_1)) = f(g(x_2)) = (f \circ g)(x_2).$$

Cum $f \circ g$ este funcție injectivă, deducem $x_1 = x_2$, deci g este funcție injectivă.

Fie $z \in E$. Dacă $f \circ g$ este funcție surjectivă, atunci există $x \in E$ astfel încît

$$z = (f \circ g)(x) = f(g(x)).$$

Rezultă că $z = f(y)$, unde $y = g(x) \in E$, deci f este funcție surjectivă.

2) Rezultă din 1) observînd că 1_E este funcție injectivă și surjectivă.

3) Rezultă din 2).

R — 2 Fie $E = \mathbf{Z} \times \mathbf{Z}$ şi $A = \begin{pmatrix} 2 & 3 \\ -1 & -2 \end{pmatrix}$. Definim funcţia :

$$f_A : E \to E, \quad f_A(x) = (2x_1 + 3x_2, \quad -x_1 - 2x_2) \qquad \forall\, x = (x_1, x_2) \in E.$$

Arătaţi că :

1) $f_A \circ f_A = 1_E$.

2) f_A este funcţie bijectivă.

Soluţie. 1) Pentru orice $x \in E$, $x = (x_1, x_2)$ avem

$$(f_A \circ f_A)(x) = f_A(f_A(x)) = f_A((2x_1 + 3x_2, -x_1 - 2x_2)) =$$
$$= (2(2x_1 + 3x_2) + 3(-x_1 - 2x_2), -(2x_1 + 3x_2) - 2(-x_1 - 2x_2)) = (x_1, x_2) = x,$$

de unde $f_A \circ f_A = 1_E$.

2) Rezultă din Ex. R-1, pct. 2).

R — 3 Fie $U, A \in M_2(\mathbf{Z})$,

$$U = \begin{pmatrix} 3 & 1 \\ 5 & 2 \end{pmatrix}, \ A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$

1) Găsiţi o matrice $X \in M_2(\mathbf{Z})$ astfel încît $UX = E$;

2) Arătaţi că ecuaţia $AX = E$ admite o soluţie $X \in M_2(\mathbf{Z})$ dacă şi numai dacă $\det(A) = \pm 1$ şi în acest caz avem şi $XA = E$.

Soluţie. 1) Fie $X = \begin{pmatrix} x & y \\ z & w \end{pmatrix}$. Cum

$$UX = \begin{pmatrix} 3 & 1 \\ 5 & 2 \end{pmatrix} \begin{pmatrix} x & y \\ z & w \end{pmatrix} = \begin{pmatrix} 3x + z & 3y + w \\ 5x + 2z & 5y + 2w \end{pmatrix}$$

avem $UX = E$ dacă şi numai dacă

$$\begin{pmatrix} 3x + z & 3y + w \\ 5x + 2z & 5y + 2w \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

ceea ce revine la :

a) $\begin{cases} 3x + z = 1 \\ 5x + 2z = 0 \end{cases}$ şi b) $\begin{cases} 3y + w = 0 \\ 5y + 2w = 1. \end{cases}$

Rezolvînd sistemele de mai sus găsim $x = 2$, $z = -5$, $y = -1$ şi $w = 3$, deci

$$X = \begin{pmatrix} 2 & -1 \\ -5 & 3 \end{pmatrix} \in M_2(\mathbf{Z}).$$

2) Fie $X \in M_2(\mathbf{Z})$ astfel încît $AX = E$.
Atunci

$$1 = \det(E) = \det(AX) = \det(A)\det(X)$$

şi cum $\det(A)$ şi $\det(X)$ sînt numere întregi, rezultă că $\det(A) = \pm 1$.

Reciproc, dacă $\det(A) = \pm 1$, atunci urmînd calea de rezolvare de la pct. 1) se găseşte :

$$X = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} \in M_2(\mathbf{Z}) \text{ dacă } ad - cb = 1$$

şi

$$X = \begin{pmatrix} -d & b \\ c & -a \end{pmatrix} \in M_2(\mathbf{Z}) \text{ dacă } ad - cb = -1.$$

În ambele cazuri avem şi $XA = E$.

R — 4 Fie m_1 și m_2 doi întregi pozitivi relativ primi, $m = m_1 m_2$ și $\mathcal{R}_m = \{0, 1, 2, \ldots, m-1\}$, $\mathcal{R}_{m_1} = \{0, 1, \ldots, m_1 - 1\}$, $\mathcal{R}_{m_2} = \{0, 1, \ldots, m_2 - 1\}$.

Dacă $a, n \in \mathbf{Z}$, $n > 0$, atunci notăm cu a mod n restul împărțirii lui a prin n.

1) Arătați că funcția

$f : \mathcal{R}_m \to \mathcal{R}_{m_1} \times \mathcal{R}_{m_2}$, $f(a) = (a \bmod m_1, a \bmod m_2)$ $\forall\, a \in \mathcal{R}_m$ este bijectivă.

2) Enumerați valorile funcției f cînd $m_1 = 4$ și $m_2 = 3$.

Soluție. 1) Mulțimea $\mathcal{R}_m$ are m elemente și mulțimea $\mathcal{R}_{m_1} \times \mathcal{R}_{m_2}$ are $m_1 m_2 = m$ elemente.

Este deci suficient să arătăm că funcția f este injectivă. Fie $a, b \in \mathcal{R}_m$ astfel încît $f(a) = f(b)$. Atunci

$$(a \bmod m_1,\ a \bmod m_2) = (b \bmod m_1,\ b \bmod m_2).$$

Rezultă că $a \bmod m_1 = b \bmod m_1$ și $a \bmod m_2 = b \bmod m_2$. Cum $a \bmod m_1 = b \bmod m_1$, deducem că a și b dau același rest prin împărțirea cu m_1, deci $m_1 | (a - b)$. Analog se deduce că $m_2 | (a - b)$. Dar $(m_1, m_2) = 1$, deci $m_1 m_2 \mid (a - b)$. Cum $|a - b| < m$, rezultă $a - b = 0$, deci $a = b$. Așadar, f este funcție injectivă.

2) În acest caz $m = 4 \times 3 = 12$, $\mathcal{R}_{12} = \{0, 1, 2, \ldots, 11\}$, $\mathcal{R}_4 = \{0, 1, 2, 3\}$ și $\mathcal{R}_3 = \{0, 1, 2\}$. Avem :

$f(0) = (0, 0)$;	$f(4) = (0, 1)$;	$f(8) = (0, 2)$;
$f(1) = (1, 1)$;	$f(5) = (1, 2)$;	$f(9) = (1, 0)$;
$f(2) = (2, 2)$;	$f(6) = (2, 0)$;	$f(10) = (2, 1)$;
$f(3) = (3, 0)$;	$f(7) = (3, 1)$;	$f(11) = (3, 2)$.

Astfel :

$$f(7) = (7 \bmod 4,\ 7 \bmod 3) = (3, 1).$$

1. Fie $f : \mathbf{Z} \to \mathbf{Z}$, $f(x) = 2x + 1$, $\forall x \in \mathbf{Z}$. Arătați că :

   1) f este funcție injectivă ;

   2) f nu este funcție surjectivă.

2. Fie $f : \mathbf{N} \to \mathbf{N}$, $f(x) = x + 1$, $\forall x \in \mathbf{N}$ și $g : \mathbf{N} \to \mathbf{N}$, $g(x) = x - 1$, $\forall x \in \mathbf{N}$, $x \neq 0$ și $g(0) = 0$.

   Arătați că :

   1) f este injectivă și nu este surjectivă ;

   2) g este surjectivă și nu este injectivă ;

   3) $g \circ f = 1_N$.

3. Pentru $a, b \in \mathbf{R}$, $a \neq 0$, definim funcția $f_{a,b} : \mathbf{R} \to \mathbf{R}$, $f_{a,b}(x) = ax + b$, $\forall x \in \mathbf{R}$.

   Arătați că :

   1) $f_{a,b}$ este funcție bijectivă ;

   2) $f_{a,b} \circ f_{c,d} = f_{ac, ad+b}$ $\forall a, b, c, d \in \mathbf{R}$, $a \neq 0$, $c \neq 0$.

   3) Pentru $a, b \in \mathbf{R}$, $a \neq 0$, găsiți $\alpha, \beta \in \mathbf{R}$ astfel încît $f_{a,b} \circ f_{\alpha,\beta} = 1_{\mathbf{R}}$.

4. Fie $A \in M_2(\mathbf{Z})$, $A = \begin{pmatrix} 3 & 1 \\ 4 & 2 \end{pmatrix}$, $E = \mathbf{Z} \times \mathbf{Z}$, $F = \mathbf{Q} \times \mathbf{Q}$,

$$f_A : E \to E,\ f_A(x) = (3x_1 + x_2,\ 4x_1 + 2x_2) \qquad \forall x = (x_1, x_2) \in E,$$

$$f_A^* : F \to F,\ f_A^*(x) = (3x_1 + x_2,\ 4x_1 + 2x_2) \qquad \forall x = (x_1, x_2) \in F.$$

Arătați că :

1) f_A este funcție injectivă și nu este surjectivă.

2) f_A^* este bijectivă.

5. Fie $A \in M_2(\mathbf{Q})$, $A = \begin{pmatrix} -1/2 & 3/2 \\ -1/2 & -1/2 \end{pmatrix}$. Arătați că :

$$A^2 + A + E = 0,\ A^3 = E.$$

6. Pentru orice $\theta \in \mathbf{R}$ definim matricele :

$$R_\theta = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix},\ S_\theta = \begin{pmatrix} \cos\theta & \sin\theta \\ \sin\theta & -\cos\theta \end{pmatrix}.$$

Arătați că :

1) $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} R_{-\theta} = S_\theta$, $R_\theta \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = S_\theta$, $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = S_0$.

2) $R_\theta R_{\theta'} = R_{\theta+\theta'}$, $R_\theta S_{\theta'} = S_{\theta+\theta'}$, $S_\theta R_{\theta'} = S_{\theta-\theta'}$,
$S_\theta S_{\theta'} = R_{\theta-\theta'}$.

3) $R_\theta R_{-\theta} = R_{-\theta} R_\theta = E$, $S_\theta S_\theta = E$.

7. Pentru o matrice $A \in M_2(\mathbf{R})$ următoarele afirmații sînt echivalente :

1) Există $a \in \mathbf{R}$ astfel încît $A = \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$,

2) $AX = XA$ oricare ar fi $X \in M_2(\mathbf{R})$.

8 1) Determinați matricele $A \in M_2(\mathbf{Z})$ cu proprietățile :

$$A^2 = E \text{ și } \det(A) = 1.$$

2) Dacă

$$B = \begin{pmatrix} a & 1+a \\ 1-a & -a \end{pmatrix},\ a \in \mathbf{Z}$$

arătați că $B^2 = E$ și $\det(B) = -1$.

9. Pentru orice $a \in \mathbf{R}$ fie matricele $U_a, V_a \in M_2(\mathbf{R})$,

$$U_a = \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix},\ V_a = \begin{pmatrix} 1 & 0 \\ a & 1 \end{pmatrix}.$$

Arătați că :

1) $U_a U_b = U_{a+b}$, $V_a V_b = V_{a+b}$, $\quad \forall\, a, b \in \mathbf{R}$;

2) $U_a U_{-a} = U_{-a} U_a = E$, $V_a V_{-a} = V_{-a} V_a = E$, $\quad \forall\, a \in \mathbf{R}$.

10. Dacă $A \in M_2(\mathbf{R})$, $A = (a_{ij})$, atunci definim matricea

$$A^T = \begin{pmatrix} a_{11} & a_{21} \\ a_{12} & a_{22} \end{pmatrix} \in M_2(\mathbf{R})$$

numită *transpusa* matricei A. Verificați că :

1) $(A + B)^T = A^T + B^T$,

2) $(AB)^T = B^T A^T$

3) $(A^T)^T = A$

oricare ar fi $A, B \in M_2(\mathbf{R})$.

4) Funcția $f : M_2(\mathbf{R}) \to M_2(\mathbf{R})$, $f(A) = A^T$, $A \in M_2(\mathbf{R})$ este bijectivă.

11. Fie $H = \left\{ A \in M_2(\mathbf{R}) \;\middle|\; A = \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix},\ a, b \in \mathbf{R},\ a \neq 0 \right\}$.

Arătați :

1) Dacă $A, B \in H$, atunci $AB \in H$.

2) Oricare ar fi $A \in H$ există $X \in H$ astfel încît $AX = E$.

Comparați rezultatele acestui exercițiu cu cele de la Ex. 3.

12. Fie $a, b_1, b_2, \ldots, b_n \in \mathbf{Z}$. Demonstrați :

1) Dacă $(a, b_i) = 1$, $1 \leqslant i \leqslant n$, atunci $(a, b_1 b_2 \ldots b_n) = 1$;

2) Dacă pentru orice $i \neq j$ avem $(b_i, b_j) = 1$ și $b_i \mid a$, $1 \leqslant i \leqslant n$, atunci $b_1 b_2 \ldots b_n$ divide pe a.

13. Dacă n este impar, arătați că $n^5 - n$ se divide prin 240.

14. 1) Determinați numerele $v \in \mathbf{Z}[\sqrt{-5}]$, $v = a + b\sqrt{-5}$, $a, b \in \mathbf{Z}$, cu proprietatea că există $z \in \mathbf{Z}[\sqrt{-5}]$ astfel încît $vz = 1$.

2) Găsiți $z \in \mathbf{Q}(\sqrt{-5})$ astfel încît $vz = 1$, unde $v = 3 - \sqrt{-5}$.

15*. Fie E o mulțime și $C_E : \mathfrak{P}(E) \to \mathfrak{P}(E)$, $C_E(X) = E \setminus X$, $\forall X \in \mathfrak{P}(E)$. Arătați că aplicația C_E are proprietățile :

1) $C_E(X \cup Y) = C_E(X) \cap C_E(Y) \qquad \forall X, Y \in \mathfrak{P}(E)$,

2) $C_E(X \cap Y) = C_E(X) \cup C_E(Y) \qquad \forall X, Y \in \mathfrak{P}(E)$,

3) $C_E \circ C_E = 1_{\mathfrak{P}(E)}$,

4) Aplicația C_E este bijectivă.

16*. Fie $A \in M_2(\mathbf{R})$, $A = (a_{ij})$, $E = \mathbf{R} \times \mathbf{R}$ și $f_A : E \to E$,

$$f_A(x) = (a_{11}x_1 + a_{12}x_2,\ a_{21}x_1 + a_{22}x_2), \qquad \forall x = (x_1, x_2) \in E.$$

Arătați că următoarele afirmații sînt echivalente :

1) f_A este bijectivă ;

2) $\det(A) \neq 0$.

17*. Pentru orice $A \in M_2(\mathbf{R})$, $A = (a_{ij})$ definim aplicația f_A ca la Ex. 16*. Arătați că :

1) $f_A = f_B \Leftrightarrow A = B$;

2) $f_A \circ f_B = f_{AB}$, $\qquad \forall A, B \in M_2(\mathbf{R})$;

3) Folosind asociativitatea compunerii funcțiilor, deduceți că $(AB)C = A(BC)$, $\forall A, B, C \in M_2(\mathbf{R})$.

18*. Determinați matricele $A \in M_2(\mathbf{Z})$ cu proprietatea : $A^2 = -E$.

19*. Fie $O_2 = \{A \in M_2(\mathbf{R}) \mid A^T A = E\}$. Arătați :

1) Dacă $A \in O_2$, atunci $\det(A) = \pm 1$;

2) Avem $A \in O_2$ și $\det(A) = 1 \Leftrightarrow \exists\, \theta \in [0, 2\pi)$ astfel încît

$$A = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}.$$

3) Avem $A \in O_2$ și $\det(A) = -1 \Leftrightarrow \exists\, \theta \in [0, 2\pi)$ astfel încît

$$A = \begin{pmatrix} \cos\theta & \sin\theta \\ \sin\theta & -\cos\theta \end{pmatrix}.$$

4) Avem $A \in O_2 \Leftrightarrow A^T A = A A^T = E$;

5) Dacă $A, B \in O_2 \Rightarrow AB \in O_2$.

20*. Fie $\mathcal{H} = \{A \in M_2(\mathbf{R}) \mid A^T = A\}$ și $\mathcal{S} = \{A \in M_2(\mathbf{R}) \mid A^T = -A\}$. Arătați că :

1) $\forall A, B \in \mathcal{H} \Rightarrow A + B \in \mathcal{H}$;

2) $\forall A, B \in \mathcal{S} \Rightarrow A + B \in \mathcal{S}$;

3) $A \in \mathcal{H} \cap \mathcal{S} \Rightarrow A = 0$;

4) $\forall A \in M_2(\mathbf{R})$ există $B \in \mathcal{H}$ și $C \in \mathcal{S}$ unic determinate cu proprietatea $A = B + C$.

21*. Dacă numerele $a, b, q, r \in \mathbf{Z}$ satisfac relația $a = bq + r$, atunci $(a, b) = (b, r)$. Deduceți că (a, b) este egal cu ultimul rest diferit de 0 din algoritmul lui Euclid pentru a și b.

22*. Fie a și b două numere întregi nenegative.

1) Arătați că $(2^a - 1, 2^b - 1) = 2^{(a, b)} - 1$;

2) Deduceți că $(2^a - 1, 2^b - 1) = 1 \Leftrightarrow (a, b) = 1$.

23*. Fie $q \in \mathbf{Z}$, $q > 0$ astfel încît $q - 3$ nu se divide prin 5. Dacă $m_1 = 2^{6q-1} - 1$, $m_2 = 2^{6q+1} - 1$, $m_3 = 2^{6q+2} - 1$, $m_4 = 2^{6q+3} - 1$, $m_5 = 2^{6q+5} - 1$, $m_6 = 2^{6q+7} - 1$, atunci $(m_i, m_j) = 1$ pentru $i \neq j$.

§ 1. NOȚIUNEA DE LEGE DE COMPOZIȚIE. EXEMPLE

Să trecem mai întîi în revistă cîteva exemple cunoscute care permit degajarea conceptului de lege de compoziție.

Pentru moment să ne fixăm atenția asupra mulțimii $\mathbf{N} = \{0, 1, 2, \ldots, n, \ldots\}$ a numerelor naturale. Operația de *adunare* a numerelor naturale ne permite să definim aplicația

$$\varphi : \mathbf{N} \times \mathbf{N} \to \mathbf{N}, \ (x, y) \to \varphi(x, y)$$

prin care facem să corespundă la orice pereche ordonată (x, y) de numere naturale un număr natural unic determinat $\varphi(x, y) = x + y$, numit *suma* lui x cu y. Astfel, $\varphi(3, 7) = 3 + 7 = 10$, $\varphi(5, 4) = 5 + 4 = 9$ etc.

Analog, folosind *înmulțirea* numerelor naturale, putem defini aplicația

$$\psi : \mathbf{N} \times \mathbf{N} \to \mathbf{N}, \ (x, y) \to \psi(x, y)$$

prin care la orice pereche ordonată (x, y) de numere naturale asociem un număr natural unic determinat $\psi(x, y) = xy$, numit *produsul* lui x cu y. Astfel $\psi(3, 7) = 3 \times 7 = 21$, $\psi(5, 4) = 5 \times 4 = 20$ etc.

Schimbînd cadrul, observații similare pot fi făcute pe mulțimea $\mathfrak{P}(E)$ a tututor părților X ale unei mulțimi date E. Putem defini aplicațiile :

$$\varphi : \mathfrak{P}(E) \times \mathfrak{P}(E) \to \mathfrak{P}(E), \ (X, Y) \to \varphi(X, Y) = X \cup Y$$

și

$$\psi : \mathfrak{P}(E) \times \mathfrak{P}(E) \to \mathfrak{P}(E), \ (X, Y) \to \psi(X, Y) = X \cap Y.$$

În viziunea aceasta, φ poartă numele de operație de *reuniune*, iar $\varphi(X, Y) = X \cup Y$ se numește *reuniunea* lui X cu Y ; ψ poartă numele de operație de *intersecție*, iar $\psi(X, Y) = X \cap Y$ se numește *intersecția* lui X cu Y.

Pentru a surprinde într-o schemă generală situații ca cele enumerate mai sus, vom considera o mulțime nevidă M și o aplicație

$$\varphi : M \times M \to M, \ (x, y) \to \varphi(x, y),$$

ignorînd natura elementelor mulțimii M, precum și legea efectivă prin care la orice pereche ordonată (x, y) de elemente din M se asociază un element unic $\varphi(x, y) \in M$. Se obține astfel noțiunea de *lege de compoziție* pe mulțimea M. Mai precis :

1.1. *Definiție*. **Fie M o mulțime nevidă. O aplicație φ definită pe produsul cartezian $M \times M$ cu valori în M,**

$$\varphi : M \times M \to M, \ (x, y) \to \varphi(x, y)$$

se numește *lege de compoziție* **pe M.**

Elementul unic determinat $\varphi(x, y) \in M$ care corespunde perechii ordonate $(x, y) \in M \times M$ prin aplicaţia φ se numeşte *compusul* lui x cu y prin legea de compoziţie φ.

O lege de compoziţie pe o mulţime M poartă încă numele de *operaţie algebrică* pe M sau *operaţie binară* pe M. Este clar că adunarea şi înmulţirea numerelor naturale sînt legi de compoziţie pe $M = \mathbf{N}$, reuniunea şi intersecţia sînt legi de compoziţie pe mulţimea $M = \mathfrak{T}(E)$ a tuturor părţilor unei mulţimi E.

Legile de compoziţie sînt date în diferite notaţii. De regulă se foloseşte fie notaţia *aditivă*, fie notaţia *multiplicativă*. În notaţia *aditivă* punem $\varphi(x, y) = x + y$. Elementul $x + y$ se numeşte *suma* lui x cu y, iar legea de compoziţie φ se numeste *adunare*. În notaţia *multiplicativă* punem $\varphi(x, y) = xy$ sau $\varphi(x, y) = x \cdot y$. Elementul xy se numeşte *produsul* lui x cu y, iar legea de compoziţie φ se numeşte *înmulţire*.

În unele cazuri, fie obligaţi de tradiţie, fie din necesitatea de a distinge între mai multe operaţii algebrice, pentru compusul $\varphi(x, y)$ al lui x cu y se folosesc încă notaţii ca :

$$x o y,\ x \wedge y,\quad x \vee y,\ x * y,\ x \oplus y,\ x \perp y,\ x \top y,\ x \Delta y \text{ etc.}$$

Exemple

1. *Adunarea şi înmulţirea matricelor.* Fie $M_2(\mathbf{R})$ mulţimea matricelor pătratice de ordin 2 cu coeficienţi din $\mathbf{R}$.

Asociind fiecărei perechi ordonate (A, B) de matrice din $M_2(\mathbf{R})$ matricea $A + B \in M_2(\mathbf{R})$ se obţine o lege de compoziţie φ pe $M_2(\mathbf{R})$,

$$\varphi : M_2(\mathbf{R}) \times M_2(\mathbf{R}) \to M_2(\mathbf{R}),\ (A, B) \to \varphi(A, B) = A + B,$$

numită *operaţia de adunare* a matricelor.

Asociind fiecărei perechi ordonate (A, B) de matrice din $M_2(\mathbf{R})$ matricea $AB \in M_2(\mathbf{R})$ se obţine o lege de compoziţie ψ pe $M_2(\mathbf{R})$,

$$\psi : M_2(\mathbf{R}) \times M_2(\mathbf{R}) \to M_2(\mathbf{R}),\ (A, B) \to \psi(A, B) = AB,$$

numită *operaţia de înmulţire* a matricelor.

2. *Compunerea funcţiilor.* Fie E o mulţime şi $\mathcal{F}(E)$ mulţimea tuturor funcţiilor $f : E \to E$. Asociind fiecărei perechi ordonate (f, g) de funcţii din $\mathcal{F}(E)$ funcţia $f o g \in \mathcal{F}(E)$ se obţine o lege de compoziţie φ pe $\mathcal{F}(E)$,

$$\varphi : \mathcal{F}(E) \times \mathcal{F}(E) \to \mathcal{F}(E), \qquad (f, g) \to \varphi(f, g) = f o g,$$

numită *operaţia de compunere* a funcţiilor.

3. *Adunarea şi înmulţirea modulo n.* Fie $\mathbf{Z}$ mulţimea numerelor întregi şi $n > 0$ un număr întreg fixat. Este ştiut că pentru orice $a \in \mathbf{Z}$ există q, $r \in \mathbf{Z}$ unic determinaţi astfel încît

$$a = nq + r,\ 0 \leqslant r < n.$$

Numărul r de mai sus, cunoscut sub numele de *restul* împărțirii lui a prin n, va fi notat cu a mod n (se citește „a modulo n") și se numește încă *redusul modulo* n al numărului întreg a. Astfel, dacă $n = 5$, atunci $13 \bmod 5 = 3$, $(-8) \bmod 5 = 2$, $4 \bmod 5 = 4$.

Dacă $a, b \in \mathbf{Z}$ atunci definim *suma modulo* n a lui a cu b, notată cu $a \oplus b$, și *produsul modulo* n al lui a cu b, notat cu $a \otimes b$, prin:

$$a \oplus b \overset{\text{def}}{=} (a + b) \bmod n,$$

respectiv

$$a \otimes b \overset{\text{def}}{=} (ab) \bmod n.$$

Avem astfel pe $\mathbf{Z}$, alături de adunarea și înmulțirea uzuală

$$\mathbf{Z} \times \mathbf{Z} \to \mathbf{Z},\ (a,\ b) \to a + b \text{ și } \mathbf{Z} \times \mathbf{Z} \to \mathbf{Z},\ (a,\ b) \to ab,$$

următoarele două legi de compoziție:

$$\varphi : \mathbf{Z} \times \mathbf{Z} \to \mathbf{Z},\ (a,\ b) \to \varphi(a,\ b) = a \oplus b$$

și

$$\psi : \mathbf{Z} \times \mathbf{Z} \to \mathbf{Z},\ (a,\ b) \to \psi(a,\ b) = a \otimes b$$

numite *adunarea modulo* n, respectiv *înmulțirea modulo* n.

Astfel, dacă $n = 6$, atunci $7 \oplus 9 = 4$, $(-3) \otimes 5 = 3$ deoarece $7 \oplus 9 = (7 + 9) \bmod 6 = 16 \bmod 6 = 4$, $(-3) \otimes 5 = ((-3) \times 5) \bmod 6 = (-15) \bmod 6 = (-3) \bmod 6 = (0-3) \bmod 6 = (6 - 3) \bmod 6 = 3$.

§ 2. PARTE STABILĂ. LEGE DE COMPOZIȚIE INDUSĂ

2.1. *Definiție.* **Fie M o mulțime pe care este definită o lege de compoziție φ. O submulțime H a lui M cu proprietatea:**

$$\forall\, x,\ y \in H \Rightarrow \varphi(x,\ y) \in H$$

se numește parte *stabilă* a lui M în raport cu legea de compoziție φ.

Dacă H este o parte stabilă a lui M în raport cu legea de compoziție $\varphi : M \times M \to M$, atunci pe H putem defini legea de compoziție $\varphi' : H \times H \to H$, punînd

$$\varphi'(x,\ y) \overset{\text{def}}{=} \varphi(x,\ y) \in H \quad \forall\, x,\ y \in H.$$

Vom spune că φ' este *legea de compoziție indusă* pe H de către φ.

Exemple

1. Mulțimea $2\mathbf{Z} = \{2k \mid k \in \mathbf{Z}\}$ a numerelor întregi pare este o parte stabilă a lui $\mathbf{Z}$ în raport cu operația de adunare a numerelor întregi pentru că suma a două numere pare este un număr par.

În adevăr, dacă $x, y \in 2\mathbf{Z}$, $x = 2h$, $y = 2k$, atunci $x + y = 2h + 2k = 2(h + k) \in 2\mathbf{Z}$.

Mulţimea $2\mathbf{Z} + 1 = \{2k + 1 \mid k \in \mathbf{Z}\}$ a numerelor întregi impare este o parte stabilă a lui $\mathbf{Z}$ în raport cu înmulţirea şi nu este parte stabilă a lui $\mathbf{Z}$ în raport cu adunarea. În adevăr, dacă $x, y \in 2\mathbf{Z} + 1$, atunci $x = 2h + 1$, $y = 2k + 1$, deci

$$xy = (2h + 1)(2k + 1) = 2(2hk + h + k) + 1 \in 2\mathbf{Z} + 1$$

şi

$$x + y = 2h + 1 + 2k + 1 = 2(h + k + 1) \notin 2\mathbf{Z} + 1.$$

2. Fie n un număr natural mai mare ca 0 şi

$$\mathcal{R}_n = \{0, 1, 2, \ldots, n - 1\} \subset \mathbf{Z}.$$

Mulţimea $\mathcal{R}_n$ este o parte stabilă a lui $\mathbf{Z}$ atît în raport cu adunarea modulo n cît şi în raport cu înmulţirea modulo n. În adevăr, oricare ar fi $x, y \in \mathbf{Z}$ avem $x \oplus y \in \mathcal{R}_n$ şi $x \otimes y \in \mathcal{R}_n$ şi în particular

$$\forall\, x, y \in \mathcal{R}_n \Rightarrow x \oplus y \in \mathcal{R}_n, \quad x \otimes y \in \mathcal{R}_n.$$

Dacă $n > 1$, atunci $\mathcal{R}_n$ nu este stabilă în raport cu adunarea numerelor întregi, iar dacă $n > 2$, atunci $\mathcal{R}_n$ nu este stabilă în raport cu înmulţirea uzuală a numerelor întregi.

3. Fie $E = \{1, 2, 3\}$ şi $H = \{f \in \mathcal{F}(E) \mid f(3) = 3\}$.
Atunci H este o parte stabilă a lui $\mathcal{F}(E)$ în raport cu operaţia de compunere. În adevăr, dacă $f, g \in H$, atunci $f(3) = 3$, $g(3) = 3$, deci

$$(f \circ g)(3) = f(g(3)) = f(3) = 3,$$

de unde $f \circ g \in H$.

§ 3. TABLA UNEI LEGI DE COMPOZIŢIE

Fie M o mulţime finită, $M = \{a_1, a_2, \ldots, a_n\}$. În acest caz o lege de compoziţie φ pe M, $\varphi : M \times M \to M$, poate fi dată prin ceea ce este cunoscut sub numele de *tabla* operaţiei φ, care constă dintr-un tabel cu n linii şi n coloane afectate celor n elemente ale lui M. Tabla legii de compoziţie φ conţine la intersecţia liniei lui a_i cu coloana lui a_j elementul $\varphi(a_i, a_j)$.

	a_1	a_2	$\ldots$	a_j	$\ldots$	a_n
a_1						
a_2						
$\vdots$						
a_i				$\varphi(a_i, a_j)$		
$\vdots$						
a_n						

Tabla unei operații este utilă în perfectarea calculelor algebrice și, așa cum se va vedea mai tîrziu, în testarea unor proprietăți ale operației.

Tablele operațiilor induse pe $\mathcal{R}_5 = \{0, 1, 2, 3, 4\}$ de adunarea și înmulțirea modulo 5 sînt următoarele :

⊕	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

Tabla adunării modulo 5.

⊗	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Tabla înmulțirii modulo 5.

Fie acum $E = \{1, 2, \ldots, n\}$. O funcție $f : E \to E$ se dă uneori cu ajutorul unui tabel cu două linii :

$$f = \begin{pmatrix} 1 & 2 \ldots n \\ f(1) & f(2) \ldots f(n) \end{pmatrix}.$$

În prima linie se trec în ordine numerele $1, 2, \ldots, n$ iar în a doua linie se trec imaginile acestora prin f, anume $f(1), f(2), \ldots, f(n)$. Astfel, dacă $E = \{1, 2\}$, atunci elementele lui $\mathcal{F}(E)$ sînt :

$$e = \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix}, \quad f = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}, \quad g = \begin{pmatrix} 1 & 2 \\ 1 & 1 \end{pmatrix}, \quad h = \begin{pmatrix} 1 & 2 \\ 2 & 2 \end{pmatrix}.$$

Tabla operației de compunere a funcțiilor din $\mathcal{F}(E)$ este următoarea :

∘	e	f	g	h
e	e	f	g	h
f	f	e	h	g
g	g	g	g	g
h	h	h	h	h

Astfel, $f \circ h = g$. În adevăr

$$(f \circ h)(1) = f(h(1)) = f(2) = 1 = g(1)$$

și

$$(f \circ h)(2) = f(h(2)) = f(2) = 1 = g(2)$$

de unde $f \circ h = g$. Rezultă că la intersecția liniei lui f cu coloana lui h din tabla operației de compunere a funcțiilor din $\mathcal{F}(E)$ se pune funcția g.

Direct din tabla operației de compunere a funcțiilor din $\mathcal{F}(E)$ se deduce că submulțimea $H = \{e, f\}$ a lui $\mathcal{F}(E)$ este stabilă în raport cu operația de compunere a funcțiilor.

§ 4. ASOCIATIVITATE

Noțiunea de lege de compoziție prezintă un mare grad de generalitate. În definiția unei legi de compoziție φ pe o mulțime M se ignoră atît natura elementelor mulțimii M cît și modul efectiv în care φ acționează pe $M \times M$. Singura restricție pusă este ca φ să asocieze la orice cuplu ordonat (x, y) de elemente din M un element $\varphi(x, y)$ din M și numai unul. Din acest motiv studiul legilor de compoziție bazat doar pe definiția lor este foarte sărac în rezultate. S-a dovedit fertilă ideea de a studia legi de compoziție ce au proprietăți care pot fi „semnalate" în multe exemple „concrete".

Vom presupune în continuare că M este o mulțime nevidă echipată cu o lege de compoziție „$*$",

$$M \times M \to M, \ (x, y) \to x*y.$$

Expresia $x*y$ se citește : x compus cu y sau x star y sau x stea y.

Definițiile și rezultatele vor fi date folosind această notație (notația „star") urmînd să fie făcute precizările ce se impun și în alte notații pentru legea de compoziție.

Fie $x, y, z \in M$. Prezența parantezelor în expresia

$$(x*y)*z$$

cere următoarea procedură de calcul : se află întîi compusul lui x cu y și apoi $x*y$ se compune (la dreapta !) cu z, obținîndu-se în final elementul $(x*y)*z \in M$. Prezența parantezelor în expresia $x*(y*z)$ impune să aflăm întîi $y*z$ și să-l compunem apoi (la stînga !) cu x, obținîndu-se astfel elementul $x*(y*z) \in M$.

4.1. ***Definiție.*** **O lege de compoziție $M \times M \to M$, $(x, y) \to x*y$, se numește *asociativă* dacă :**

$$(x*y)*z = x*(y*z), \qquad \forall\, x, y, z \in M.$$

Dacă legea de compoziție este dată în notație aditivă (multiplicativă) atunci proprietatea de asociativitate a acesteia se scrie :

$$(x + y) + z = x + (y + z), \ \forall\, x, y, z \in M,$$

respectiv

$$(xy)z = x(yz), \ \forall\, x, y, z \in M.$$

Dacă folosim notația $x \perp y$ pentru compusul lui x cu y, atunci proprietatea de asociativitate se scrie :

$$(x \perp y) \perp z = x \perp (y \perp z), \ \forall\, x, y, z \in M.$$

Exemple

1. Adunarea și înmulțirea numerelor reale sînt legi de compoziție asociative pentru că

$$(x + y) + z = x + (y + z), \quad (xy)z = x(yz), \ \forall\, x, y, z \in \mathbf{R}.$$

2. Adunarea și înmulțirea matricelor din $M_2(\mathbf{R})$ sînt legi de compoziție asociative, deoarece

$$(A + B) + C = A + (B + C), \ (AB)C = A(BC), \ \forall\, A, B, C \in M_2(\mathbf{R}).$$

3. Reuniunea și intersecția părților unei mulțimi E sînt legi de compoziție asociative, deoarece

$$(X \cup Y) \cup Z = X \cup (Y \cup Z), \quad (X \cap Y) \cap Z = X \cap (Y \cap Z)$$

oricare ar fi $X, Y, Z \in \mathfrak{P}(E)$.

4. Compunerea funcțiilor unei mulțimi E în ea însăși este o lege de compoziție asociativă, deoarece

$$(f \circ g) \circ h = f \circ (g \circ h), \ \forall\, f, g, h \in \mathfrak{F}(E).$$

5. Pe mulțimea $\mathbf{Z}$ a numerelor întregi definim legea de compoziție

$$\mathbf{Z} \times \mathbf{Z} \to \mathbf{Z}, \quad (x, y) \to x - y.$$

Cum $(3 - 7) - 1 = -5 \neq -3 = 3 - (7 - 1)$, rezultă că această lege de compoziție nu este asociativă.

§ 5. COMUTATIVITATE

Proprietatea de asociativitate lărgește mult aria posibilităților în perfectarea calculului algebric. O altă sursă în acest sens este dată de legile de compoziție pentru care compusul a două elemente oarecare este independent de ordinea în care se face compunerea acestora. Mai precis :

5.1. *Definiție.* **O lege de compoziție $M \times M \to M$, $(x, y) \to x*y$ se numește *comutativă*, dacă :**

$$x*y = y*x, \ \forall\, x, y \in M.$$

Adunarea și înmulțirea numerelor reale, reuniunea și intersecția părților unei mulțimi sînt legi de compoziție comutative.

Remarcă. Comutativitatea unei legi de compoziție dată pe o mulțime finită M poate fi verificată pe tabla operației : elementul xy de la intersecția liniei lui x cu coloana lui y trebuie să fie egal cu elementul yx de la intersecția liniei lui y cu coloana lui x, oricare

ar fi $x, y \in M$. Aceasta revine la proprietatea că tabla operației este simetrică în raport cu diagonala principală (fig. II.1).

În § 3 au fost date tablele adunării și înmulțirii modulo 5 pe $\mathcal{R}_5 = \{0, 1, 2, 3, 4\}$. Cum aceste table sînt simetrice în raport cu diagonala principală, rezultă că legile de compoziție menționate sînt comutative. Tot la locul citat a fost dată tabla compunerii funcțiilor din $\mathcal{F}(E)$, unde $E = \{1, 2\}$. Pe tabla acestei legi de compoziție se constată că $h \circ g = h \neq g = g \circ h$, deci această operație nu este comutativă.

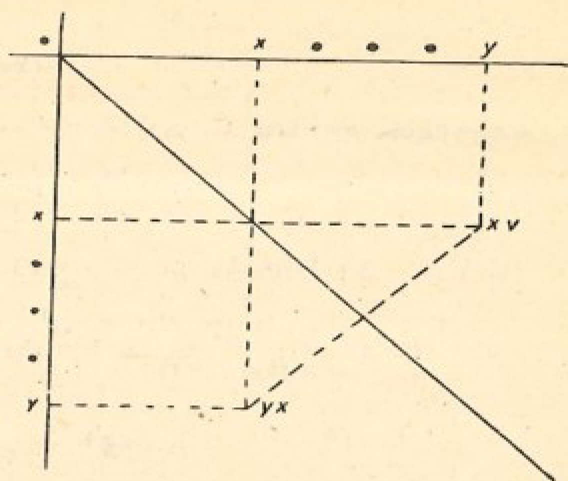


Fig. II.1.

Numeroase legi de compoziție se definesc cu ajutorul altora deja cunoscute. Asemenea operații pot prelua unele proprietăți de la cele de plecare prin „mecanismul" dat chiar de definiția lor. Astfel comutativitatea adunării matricelor din $M_2(\mathbf{R})$ este o consecință a proprietății de comutativitate a adunării numerelor reale. În adevăr, dacă $A, B \in M_2(\mathbf{R})$, $A = (a_{ij})$, $B = (b_{ij})$, atunci

$$A + B = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} + \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix} = \begin{pmatrix} a_{11} + b_{11} & a_{12} + b_{12} \\ a_{21} + b_{21} & a_{22} + b_{22} \end{pmatrix} =$$

$$= \begin{pmatrix} b_{11} + a_{11} & b_{12} + a_{12} \\ b_{21} + a_{21} & b_{22} + a_{22} \end{pmatrix} = \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix} + \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} = B + A.$$

Să observăm că înmulțirea matricelor din $M_2(\mathbf{R})$ nu este comutativă, cu toate că înmulțirea numerelor reale este comutativă. Aceasta rezultă din exemplul următor:

$$\begin{pmatrix} 1 & 2 \\ -1 & 0 \end{pmatrix}\begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 2 & 1 \\ 0 & 1 \end{pmatrix} \neq \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix} = \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}\begin{pmatrix} 1 & 2 \\ -1 & 0 \end{pmatrix}.$$

Exerciții rezolvate

R — 1 Pe mulțimea **Z** a numerelor întregi definim legea de compoziție

$$\mathbf{Z} \times \mathbf{Z} \to \mathbf{Z}, \quad (x, y) \to x \circ y \overset{\text{def}}{=} x + y - xy,$$

numită *compunerea circulară*. Să se arate că legea de compoziție „o" este asociativă și comutativă.

Soluție. Dacă $x, y, z \in \mathbf{Z}$, atunci:

$$(x \circ y) \circ z = (x + y - xy) \circ z = x + y - xy + z - (x + y - xy)z =$$
$$= x + y + z - xy - yz - zx + xyz,$$
$$x \circ (y \circ z) = x \circ (y + z - yz) = x + y + z - yz - x(y + z - yz) =$$
$$= x + y + z - xy - yz - zx + xyz,$$

de unde

$$(x o y) o z = x o (y o z).$$

De asemenea, pentru $x, y \in \mathbf{Z}$ avem:

$$x o y = x + y - xy = y + x - yx = y o x.$$

R — 2 Fie M şi N două mulţimi, „$*$" o lege de compoziţie pe M, „o" o lege de compoziţie pe N şi $f : M \to N$ o funcţie surjectivă astfel încît

$$f(x*y) = f(x) o f(y), \qquad \forall\, x, y \in M.$$

1) Dacă legea de compoziţie „$*$" este asociativă (comutativă) atunci legea de compoziţie „o" este asociativă (resp. comutativă).

2) Funcţia $f : \mathbf{Z} \to \mathbf{Z}$, $f(x) = 1 - x$ are proprietatea

$$f(xy) = f(x) o f(y), \qquad \forall\, x, y \in \mathbf{Z}$$

unde xy este produsul uzual în $\mathbf{Z}$ iar „o" este compunerea circulară (v. Ex. R — 1).

3) Daţi o nouă soluţie pentru Ex. R — 1.

Soluţie. 1) Fie $u, v, w \in N$. Cum f este funcţie surjectivă, există $x, y, z \in M$ astfel încît $u = f(x)$, $v = f(y)$, $w = f(z)$.
Avem:

$$u o v = f(x) o f(y) = f(x * y) = f(y * x) = f(y) o f(x) = v o u$$

şi

$$(u o v) o w = (f(x) o f(y)) o f(z) = f(x * y) o f(z) = f((x * y) * z) =$$

$$= f(x * (y * z)) = f(x) o f(y * z) = f(x) o (f(y) o f(z)) = u o (v o w).$$

2) Oricare ar fi $x, y \in \mathbf{Z}$ avem:

$$f(x) o f(y) = f(x) + f(y) - f(x)f(y) = 1 - x + 1 - y - (1 - x)(1 - y) =$$

$$= 1 - xy = f(xy).$$

3) Funcţia f este surjectivă iar înmulţirea uzuală a numerelor întregi este asociativă şi comutativă. Putem aplica 1).

5.2. *Remarcă.* Fie $\varphi : M \times M \to M$ o lege de compoziţie pe M, H o parte stabilă a lui M în raport cu φ şi φ' legea de compoziţie pe H indusă de φ.

Dacă φ este asociativă (comutativă) atunci φ' este asociativă (respectiv comutativă). În adevăr, pentru orice $x, y, z \in H$ avem:

$$\varphi'(\varphi'(x, y), z)) = \varphi(\varphi(x, y), z)) = \varphi(x, \varphi(y, z)) = \varphi'(x, \varphi'(y, z))$$

şi

$$\varphi'(x, y) = \varphi(x, y) = \varphi(y, x) = \varphi'(y, x).$$

§ 6. ELEMENT NEUTRU

Numerele reale 0 şi 1 au proprietăţile :

$$0 + x = x + 0 = x, \quad \forall\, x \in \mathbf{R},$$

respectiv

$$1 \cdot x = x \cdot 1 = x, \quad \forall\, x \in \mathbf{R}.$$

Dacă E este o mulţime şi $1_E : E \to E$ este aplicaţia identică a lui E, atunci

$$1_E \circ f = f \circ 1_E = f, \quad \forall\, f \in \mathcal{F}(E).$$

De asemenea, pentru orice $A \in M_2(\mathbf{R})$ avem :

$$0 + A = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} = \begin{pmatrix} 0 + a_{11} & 0 + a_{12} \\ 0 + a_{21} & 0 + a_{22} \end{pmatrix} = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} = A$$

şi analog $A + 0 = A$.

6.1. *Definiţie.* **Un element** $e \in M$ **se numeşte** *element neutru* **pentru o lege de compoziţie** $M \times M \to M, (x, y) \to x * y$, **dacă**

$$e * x = x * e = x, \quad \forall\, x \in M.$$

6.2. **T e o r e m ă. Dacă o lege de compoziţie are element neutru, atunci acesta este unic.**

Demonstraţie. Fie e şi e' două elemente neutre pentru o lege de compoziţie $M \times M \to M$, $(x, y) \to x * y$. Avem $e * e' = e'$ căci e este element neutru. De asemenea, $e * e' = e$ căci şi e' este element neutru, de unde $e = e'$.

Aşadar, elementul neutru, în caz că există, este unic determinat.

În notaţie aditivă elementul neutru se notează, de regulă cu 0 şi se numeşte *elementul zero*, iar în notaţia multiplicativă elementul neutru se notează cu 1 sau chiar cu e şi poartă numele de *elementul unitate*. Avem :

$$0 + x = x + 0 = x, \quad \forall\, x \in M,$$

respectiv

$$1 \cdot x = x \cdot 1 = x, \quad \forall\, x \in M.$$

Exemple

1. Numărul real 0 este elementul neutru al adunării numerelor reale, numărul real 1 este elementul neutru al înmulţirii numerelor reale.
2. Aplicaţia identică 1_E a mulţimii E este elementul neutru al operaţiei de compunere a funcţiilor din $\mathcal{F}(E)$.
3. Fie E o mulţime. Cum $\varnothing \cup X = X \cup \varnothing = X$ şi $E \cap X = X \cap E = X$ oricare ar fi $X \in \mathcal{P}(E)$ rezultă că $\varnothing$ este elementul neutru al operaţiei „$\cup$", iar E este elementul neutru al operaţiei „$\cap$".

4. Mulţimea $2\mathbf{N} = \{2k \mid k \in \mathbf{N}\}$ a numerelor naturale pare este o parte stabilă a lui $\mathbf{N}$ în raport cu înmulţirea şi legea de compoziţie indusă de către aceasta pe $2\mathbf{N}$ nu admite element neutru.

§ 7. ELEMENTE SIMETRIZABILE

Ca şi pînă acum, M este o mulţime nevidă înzestrată cu o lege de compoziţie

$$M \times M \to M, \quad (x, y) \to x*y.$$

Vom presupune în plus că această lege de compoziţie este asociativă şi că admite element neutru, fie acesta e.

7.1. *Definiţie.* **Un element $x \in M$ se numeşte *simetrizabil* în raport cu legea de compoziţie (asociativă şi cu element neutru) $M \times M \to M$, $(x, y) \to x*y$, dacă există $x' \in M$ astfel încît**

$$x'*x = x*x' = e.$$

Să observăm că dacă $x'' \in M$ satisface ca şi x' condiţiile

$$x''*x = x*x'' = e,$$

atunci $x' = x''$. În adevăr

$$x' = x'*e = x'*(x*x'') = (x'*x)*x'' = e*x'' = x''.$$

Dacă $x \in M$ este simetrizabil, atunci unicul element $x' \in M$ cu proprietatea $x'*x = x*x' = e$ se numeşte *simetricul* lui x (în raport cu operaţia „$*$").

În notaţia multiplicativă simetricul lui x, în caz că există, se notează de regulă cu x^{-1} şi se numeşte *inversul* lui x ; în notaţia aditivă se notează cu $-x$ şi se numeşte *opusul* lui x. Aşadar,

$$x^{-1}x = xx^{-1} = 1,$$

respectiv

$$(-x) + x = x + (-x) = 0.$$

Exemple

1. Cum $e*e = e$, rezultă că elementul neutru este simetrizabil şi simetricul lui e este tot e. În notaţie multiplicativă avem $1^{-1} = 1$, iar în notaţie aditivă $-0 = 0$.

2. Matricea $A \in M_2(\mathbf{Z})$, $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ cu $ad - cb = 1$, este simetrizabilă (inversabilă) în raport cu operaţia de înmulţire din $M_2(\mathbf{Z})$ şi

$$A^{-1} = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} \in M_2(\mathbf{Z}).$$

În adevăr,

$$\begin{pmatrix} d & -b \\ -c & a \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix}=\begin{pmatrix} ad-bc & 0 \\ 0 & -cb+ad \end{pmatrix}=\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}=E$$

și analog

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} d & -b \\ -c & a \end{pmatrix}=\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}=E.$$

3. Orice număr întreg este simetrizabil în raport cu adunarea numerelor întregi; numerele întregi simetrizabile față de înmulțire sînt 1 și -1, $1^{-1}=1$, $(-1)^{-1}=-1$.

4. Consultînd tabla dată la § 3 pentru compunerea funcțiilor din $\mathcal{F}(E)$, unde $E=\{1, 2\}$, se observă că $e\circ e=e$ și $f\circ f=e$, deci funcțiile e și f sînt simetrizabile (inversabile) și $e^{-1}=e$, $f^{-1}=f$.

7.2. **Teoremă. Dacă $x, y \in M$ sînt elemente simetrizabile în raport cu o lege de compoziție $M\times M\to M$, $(x, y)\to x*y$ (asociativă și cu element neutru) atunci $x*y$ și x' sînt simetrizabile. Mai mult:**

1) $(x*y)'=y'*x'$,

2) $(x')'=x$.

Demonstrație. Avem:

$$(y'*x')*(x*y)=y'*(x'*(x*y))=y'*((x'*x)*y)=$$
$$=y'*(e*y)=y'*y=e$$

și analog $(x*y)*(y'*x')=e$. Rezultă că $x*y$ este simetrizabil și $(x*y)'=y'*x'$. A doua afirmație este imediată.

Proprietățile 1) și 2) din enunțul teoremei precedente se transcriu multiplicativ astfel:

$$(xy)^{-1}=y^{-1}x^{-1},\quad (x^{-1})^{-1}=x,$$

iar în notația aditivă

$$-(x+y)=(-y)+(-x),\quad -(-x)=x.$$

Se face următoarea convenție de notație:

$$\boxed{x-y\overset{\text{def}}{=}x+(-y)}$$

Exerciții rezolvate

R — 1 Să se arate că legea de compoziție

$$\mathbf{Z}\times\mathbf{Z}\to\mathbf{Z},\ (x, y)\to x\circ y=x+y-xy$$

are element neutru şi să se determine elementele simetrizabile. Aceeaşi problematică pentru legea de compoziţie

$$\mathbf{Q} \times \mathbf{Q} \to \mathbf{Q},\ (x,\ y) \to x \circ y = x + y - xy.$$

Soluţie. Dacă $e \in \mathbf{Z}$ este element neutru pentru legea de compoziţie „o", trebuie să avem

$$x = e \circ x = e + x - ex,\ \forall x \in \mathbf{Z}$$

deci

$$e = ex,\quad \forall x \in \mathbf{Z}$$

şi în particular $e = e \cdot 0 = 0$. Pe de altă parte se verifică că $0 \circ x = x \circ 0 = x$, $\forall x \in \mathbf{Z}$, deci numărul 0 este elementul neutru al legii de compoziţie „o".

Fie $a \in \mathbf{Z}$. Pentru ca a să fie simetrizabil în raport cu legea de compoziţie „o" trebuie să existe $x \in \mathbf{Z}$ astfel încît

$$0 = a \circ x = a + x - ax,$$

de unde

$$x(a - 1) = a.$$

Se observă că această ecuaţie admite o soluţie $x \in \mathbf{Z}$ dacă şi numai dacă $a = 0$ sau $a = 2$. Elementele simetrizabile sînt 0 şi 2, $0' = 0$ şi $2' = 2$.

Cînd $\mathbf{Z}$ se înlocuieşte cu $\mathbf{Q}$, elementele simetrizabile sînt toate numerele raţionale $a \neq 1$.

R — 2 Fie d un număr întreg liber de pătrate şi

$$H = \left\{ A \in M_2(\mathbf{Q}) \;\middle|\; A = \begin{pmatrix} a & db \\ b & a \end{pmatrix},\ a,\ b \in \mathbf{Q},\ a \neq 0 \text{ sau } b \neq 0 \right\}.$$

1) H este o parte stabilă a lui $M_2(\mathbf{Q})$ în raport cu înmulţirea matricelor.

2) Orice matrice $A \in H$ este inversabilă (simetrizabilă) în raport cu operaţia indusă.

Soluţie. 1) Fie $A,\ B \in H$, $A = \begin{pmatrix} a & bd \\ b & a \end{pmatrix}$, $B = \begin{pmatrix} a' & db' \\ b' & a' \end{pmatrix}$.

Avem

$$AB = \begin{pmatrix} aa' + dbb' & d(ba' + ab') \\ ba' + ab' & aa' + dbb' \end{pmatrix} = \begin{pmatrix} a'' & db'' \\ b'' & a'' \end{pmatrix}$$

unde $a'' = aa' + dbb' \in \mathbf{Q}$, $b'' = ba' + ab' \in \mathbf{Q}$. Pentru a avea $AB \in H$ este suficient să arătăm că $a'' \neq 0$ sau $b'' \neq 0$. Dacă $a'' = 0$ şi $b'' = 0$ atunci $x = a'$ şi $y = b'$ este o soluţie nebanală a sistemului omogen:

$$(*) \begin{cases} ax + dby = 0, \\ bx + ay = 0. \end{cases}$$

Determinantul matricei acestui sistem este egal cu $a^2 - db^2$. Cum d este liber de pătrate şi $a \neq 0$ sau $b \neq 0$, rezultă că $a^2 - db^2 \neq 0$ căci altfel $\sqrt{d} \in \mathbf{Q}$ Contradicţie. Dar din $a^2 - db^2 \neq 0$ rezultă că singura soluţie a sistemului $(*)$ este $x = y = 0$. Rămîne adevărat că $a'' \neq 0$ sau $b'' \neq 0$, deci $AB \in H$.

2) Se observă că matricea unitate $E \in H$ şi fie $A \in H$. Să arătăm că există o matrice $X \in H$,

$$X = \begin{pmatrix} x & dy \\ y & x \end{pmatrix},\ x,\ y \in \mathbf{Q},\ x \neq 0 \text{ sau } y \neq 0$$

astfel încît $XA = AX = E$. Avem :

$$\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix} = E = AX = \begin{pmatrix}a & db\\ b & a\end{pmatrix}\begin{pmatrix}x & dy\\ y & x\end{pmatrix} = \begin{pmatrix}ax + dby & d(bx+ay)\\ bx + ay & ax + dby\end{pmatrix}$$

ceea ce este echivalent cu sistemul liniar :

$$(**)\begin{cases}ax + dby = 1,\\ bx + ay = 0.\end{cases}$$

Determinantul sistemului $(**)$ este $a^2 - db^2 \neq 0$ și unica soluție este $x = a/(a^2 - db^2)$, $y = -b/(a^2 - db^2)$.

Cum $a \neq 0$ sau $b \neq 0$, rezultă $x \neq 0$ sau $y \neq 0$. Așadar :

$$X = \begin{pmatrix}\dfrac{a}{a^2 - db^2} & \dfrac{-db}{a^2 - db^2}\\ \dfrac{-b}{a^2 - db^2} & \dfrac{a}{a^2 - db^2}\end{pmatrix} \in H.$$

Se verifică și egalitatea $XA = E$, deci A^{-1} există și $A^{-1} = X \in H$.

§ 8. PROPRIETĂȚI ALE ADUNĂRII ȘI ÎNMULȚIRII MODULO n

În capitolul I, § 1, au fost enumerate proprietățile adunării și înmulțirii numerelor întregi.

Anume, cu terminologia adoptată în capitolul de față, adunarea numerelor întregi,

$$\mathbf{Z} \times \mathbf{Z} \to \mathbf{Z},\ (x,\ y) \to x + y$$

este asociativă, comutativă, admite pe 0 ca element neutru și orice număr întreg admite opus.

De asemenea, înmulțirea numerelor întregi

$$\mathbf{Z} \times \mathbf{Z} \to \mathbf{Z}\quad (x,\ y) \to xy,$$

este asociativă, comutativă și admite pe 1 ca element neutru.

În fine, înmulțirea numerelor întregi este *distributivă* față de adunare :

$$x(y + z) = xy + xz, \qquad \forall\, x,\ y,\ z \in \mathbf{Z}.$$

Fie $n > 0$ un număr întreg. Dacă $a,\ b \in \mathbf{Z}$ am definit *suma modulo n* a lui a cu b, notată cu $a \oplus b$ și *produsul modulo n* al lui a cu b, notat cu $a \otimes b$ ca fiind restul împărțirii prin n al numărului $a + b$, respectiv ab :

$$a \oplus b \overset{\text{def}}{=\!=} (a + b) \bmod n, \qquad a \otimes b \overset{\text{def}}{=\!=} (ab) \bmod n.$$

S-au obținut astfel două legi de compoziție pe $\mathbf{Z}$,

$$\mathbf{Z} \times \mathbf{Z} \to \mathbf{Z},\quad (a,\ b) \to a \oplus b \quad \text{și} \quad \mathbf{Z} \times \mathbf{Z} \to \mathbf{Z},\ (a,\ b) \to a \otimes b$$

numite *adunarea modulo n*, respectiv *înmulțirea modulo n*.

Ne propunem în continuare să studiem proprietățile acestora. Un rezultat util pentru acest studiu este următorul :

8.1. Lemă. Fie $a, b \in \mathbf{Z}$. Atunci oricare ar fi $h, k \in \mathbf{Z}$ avem :

$$(a + nh) \oplus (b + nk) = a \oplus b$$

$$(a + nh) \otimes (b + nk) = a \otimes b.$$

Demonstrație. Pentru orice h și $k \in \mathbf{Z}$ avem :

$$(a + nh) + (b + nk) = (a + b) + n(h + k)$$

și

$$(a + nh)(b + nk) = ab + n(ak + bh + nhk).$$

Rezultă că numerele $(a + nh) + (b + nk)$ și $a + b$ dau același rest prin împărțirea cu n, deci

$$(a + nh) \oplus (b + nk) = a \oplus b$$

și, de asemenea, numerele $(a + nh)(b + nk)$ și ab dau același rest prin împărțirea cu n, deci

$$(a + nh) \otimes (b + nk) = a \otimes b.$$

8.2. Teoremă. Operațiile de adunare și înmulțire modulo n au proprietățile :

1) $(a \oplus b) \oplus c = a \oplus (b \oplus c)$,
2) $a \oplus b = b \oplus a$,
3) $(a \otimes b) \otimes c = a \otimes (b \otimes c)$,
4) $a \otimes b = b \otimes a$,
5) $a \otimes (b \oplus c) = a \otimes b \oplus a \otimes c$

oricare ar fi $a, b, c \in \mathbf{Z}$.

Demonstrație 1) Cum $a \oplus b$ este restul împărțirii lui $a + b$ prin n, există $q \in \mathbf{Z}$ astfel încît

$$a + b = nq + (a \oplus b).$$

Din lema precedentă rezultă :

$$(a \oplus b) \oplus c = (a + b) \oplus c = ((a + b) + c) \bmod n.$$

De asemenea :

$$a \oplus (b \oplus c) = a \oplus (b + c) = (a + (b + c)) \bmod n.$$

Dar $(a + b) + c = a + (b + c)$, de unde $(a \oplus b) \oplus c = a \oplus (b \oplus c)$.

4) Avem :

$$a \otimes b = (ab) \bmod n = (ba) \bmod n = b \otimes a.$$

5) Aplicînd lema 8.1 avem :

$$a \otimes (b \oplus c) = a \otimes (b + c) = (a(b + c)) \bmod n = (ab + ac) \bmod n =$$
$$= ab \oplus ac = a \otimes b \oplus a \otimes c.$$

Proprietatea 2) se demonstrează ca 4), iar 3) ca 1).

Să observăm că adunarea modulo n nu admite element neutru. În adevăr, să presupunem că $\theta \in \mathbf{Z}$ este astfel încît $\theta \oplus a = a \oplus \theta = a, \forall a \in \mathbf{Z}$. Dacă $a \notin \mathcal{R}_n = \{0, 1, 2, \ldots, n - 1\}$, atunci $\theta \oplus a \neq a$ pentru că $\theta \oplus a \in \mathcal{R}_n$. Contradicţie.

Analog se arată că înmulţirea modulo n nu admite element neutru.

Aşa cum s-a mai observat, avem:

$$\forall a, b \in \mathcal{R}_n \Rightarrow a \oplus b \in \mathcal{R}_n, \quad a \otimes b \in \mathcal{R}_n.$$

Putem deci considera operaţiile induse pe $\mathcal{R}_n$ de către operaţiile de adunare şi înmulţire modulo n,

$$\mathcal{R}_n \times \mathcal{R}_n \to \mathcal{R}_n, \qquad (a, b) \to a \oplus b$$

respectiv

$$\mathcal{R}_n \times \mathcal{R}_n \to \mathcal{R}_n, \qquad (a, b) \to a \otimes b.$$

Aceste operaţii au evident proprietăţile 1) —5) din enunţul Teoremei 8.2 (v. Remarca 5.2). Cum:

$$0 \oplus a = a \oplus 0 = a, \qquad 1 \otimes a = a \otimes 1 = a. \qquad \forall a \in \mathcal{R}_n$$

rezultă că numerele 0 şi 1 sînt elemente neutre pentru operaţiile induse pe $\mathcal{R}_n$ de către adunarea modulo n, respectiv înmulţirea modulo n.

În fine să mai observăm că

$$a \oplus (n - a) = (n - a) \oplus a = 0, \qquad \forall a \in \mathcal{R}_n$$

şi cum $n - a \in \mathcal{R}_n$ oricare ar fi $a \in \mathcal{R}_n, a \neq 0$, rezultă că orice element $a \in \mathcal{R}_n$ este simetrizabil în raport cu operaţia indusă pe $\mathcal{R}_n$ de către adunarea modulo n, simetricul (opusul) lui a fiind $n - a$ dacă $a \neq 0$ şi 0 dacă $a = 0$.

Fie $n = 6$. Tablele operaţiilor induse pe $\mathcal{R}_6 = \{0, 1\ 2, 3, 4, 5\}$ de către adunarea şi înmulţirea modulo 6 sînt:

$\oplus$	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

Tabla adunării modulo 6.

$\otimes$	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

Tabla înmulţirii modulo 6.

Faptul că operaţia indusă pe $\mathcal{R}_6$ de adunarea modulo 6 este comutativă şi că admite pe 0 ca element neutru se constată şi pe tabla acesteia. Folosind notaţia aditivă pentru simetric, se constată de asemenea că:

$$-0 = 0, \quad -1 = 5, \quad -2 = 4, \quad -3 = 3, \quad -4 = 2, \quad -5 = 1$$

căci

$$0 \oplus 0 = 0, \quad 1 \oplus 5 = 0, \quad 2 \oplus 4 = 0, \quad 3 \oplus 3 = 0.$$

Elementele din $\mathcal{R}_6$ simetrizabile în raport cu operația indusă de înmulțirea modulo 6 sînt 1 și 5. Folosind în acest caz notația multiplicativă pentru simetric, avem :

$$1^{-1} = 1, \qquad 5^{-1} = 5$$

căci $1 \otimes 1 = 1$, $5 \otimes 5 = 1$.

Remarcă. Operația „$\otimes$" are prioritate față de „$\oplus$" și de aceea într-o expresie ca $(c \otimes b) \oplus c$ parantezele pot fi omise, scriind simplu $a \otimes b \oplus c$.

Exerciții rezolvate

R — 1 Găsiți soluțiile din $\mathcal{R}_6$ ale ecuațiilor :

1) $5 \otimes x \oplus 2 = 4$,
2) $3 \otimes x \oplus 4 = 4$,
3) $2 \otimes x \oplus 3 = 2$,

unde „$\oplus$" și „$\otimes$" sînt simbolurile adunării și înmulțirii modulo 6.

Soluție. 1) Cum $5 \otimes x \oplus 2 \oplus 4 = 4 \oplus 4$ iar $2 \oplus 4 = 0$ și $4 \oplus 4 = 2$, rezultă că

$$5 \otimes x = 2.$$

Din tabla înmulțirii modulo 6 rezultă că $x = 4$. Același rezultat se obține observînd că 5 este simetrizabil în raport cu „$\otimes$" și $5^{-1} = 5$. Deducem :

$$x = 1 \otimes x = (5 \otimes 5) \otimes x = 5 \otimes (5 \otimes x) = 5 \otimes 2 = 4.$$

2) Cum $3 \otimes x \oplus 4 \oplus 2 = 4 \oplus 2$, rezultă că $3 \otimes x = 0$.
Din tabla înmulțirii modulo 6, găsim pentru x valorile $x_1 = 0$, $x_2 = 2$ și $x_3 = 4$. (O ecuație de grad 1 admite trei soluții !).

3) Cum $2 \otimes x \oplus 3 \oplus 3 = 2 \oplus 3$, rezultă $2 \otimes x = 5$. Din tabla înmulțirii modulo 6 se constată că nu există $x \in \mathcal{R}_6$ astfel încît $2 \otimes x = 5$. Așadar ecuația 3) nu admite soluții.

R — 2 1) Rezolvați în $\mathcal{R}_5$ ecuația $2 \otimes x \oplus 3 = 2$.

2) Arătați că ecuația $a \otimes x \oplus b = 0$ cu $a, b \in \mathcal{R}_5$, $a \neq 0$, admite o soluție unică în $\mathcal{R}_5$.

Soluție. 1) Adunînd la fiecare termen al ecuației opusul lui 3 în raport cu adunarea modulo 5 pe $\mathcal{R}_5$, se obține :

$$2 \otimes x \oplus 3 \oplus 2 = 2 \oplus 2,$$

deci

$$2 \otimes x = 4.$$

Din tabla înmulțirii modulo 5 pe $\mathcal{R}_5$ se constată că 2 este simetrizabil și simetricul lui 2 în raport cu această operație este 3. Înmulțind cu 3 ecuația $2 \otimes x = 4$ se obține

$$3 \otimes 2 \otimes x = 3 \otimes 4$$

și cum $3 \otimes 2 = 1$, $3 \otimes 4 = 2$, deducem că $x = 2$.

2) Consultînd tablele înmulțirii și adunării modulo 5 pe $\mathcal{R}_5 = \{0, 1, 2, 3, 4\}$ (v. § 3) se constată că toate elementele $b \in \mathcal{R}_5$ sînt simetrizabile în raport cu adunarea modulo 5 și că toate elementele $a \in \mathcal{R}_5$, $a \neq 0$, sînt simetrizabile în raport cu înmulțirea modulo 5. Așadar etapele de rezolvare de la pct. 1) pot fi parcurse și pe cazul general $a \otimes x \oplus b = 0$, $a \neq 0$, deci ecuația $a \otimes x \oplus b = 0$ are cel puțin o soluție în $\mathcal{R}_5$.

Fie $x_1, x_2 \in \mathcal{R}_5$ astfel încît $a \otimes x_1 \oplus b = 0$ și $a \otimes x_2 \oplus b = 0$. Atunci avem:

$$a \otimes x_1 \oplus b = a \otimes x_2 \otimes b.$$

Adunînd opusul lui b la fiecare termen al egalității precedente obținem

$$a \otimes x_1 = a \otimes x_2$$

și înmulțind termenii acestei ultime egalități cu simetricul lui a în raport cu înmulțirea modulo 5 se obține $x_1 = x_2$.

Exerciții

1. Să se alcătuiască tablele operațiilor induse pe $\mathcal{R}_4 = \{0, 1, 2, 3\} \subset \mathbf{Z}$ de adunarea și înmulțirea modulo 4.

2. Arătați că mulțimea $H = \{0, 1, 2, 3, 4\} \subset \mathbf{Z}$ este stabilă față de legea de compoziție $\mathbf{Z} \times \mathbf{Z} \to \mathbf{Z}$, $(x, y) \to |x - y|$ și să se alcătuiască tabla operației induse.

3. Arătați că orice submulțime $H \neq \varnothing$ a lui $\mathbf{R}$ este stabilă în raport cu fiecare din legile de compoziție

$$\alpha \perp \beta \overset{\text{def}}{=\!=} \max\{\alpha, \beta\};\ \alpha \top \beta \overset{\text{def}}{=\!=} \min\{\alpha, \beta\},\ \forall\, \alpha, \beta \in \mathbf{R}.$$

Alcătuiți tablele operațiilor induse pe $H = \{\alpha, \beta, \gamma\}$, unde

$$\alpha = \sqrt{5}, \quad \beta = \sqrt{1 + \sqrt{2}}, \quad \gamma = \sqrt[3]{3 + \sqrt{2}}.$$

4. Fie $H = \{a \in \mathbf{N} \mid a \mid 12\}$. Arătați că H este o parte stabilă a lui $\mathbf{N}$ în raport cu fiecare din legile de compoziție:

$$a \perp b \overset{\text{def}}{=\!=} \text{c.m.m.d.c.}\ \{a, b\},\ a \top b \overset{\text{def}}{=\!=} \text{c.m.m.m.c.}\ \{a, b\},\ \forall\, a, b \in \mathbf{N}.$$

Alcătuiți tablele operațiilor induse.

5. Pentru care valori ale parametrului real λ intervalul $(2, \infty)$ este o parte stabilă a lui $\mathbf{R}$ în raport cu legea de compoziție

$$x * y \overset{\text{def}}{=\!=} xy - 2x - 2y + \lambda,\ \forall\, x, y \in \mathbf{R}.$$

6. Fie $E = \mathbf{R} \setminus \{-\sqrt{3}/3, \sqrt{3}/3\}$ și $f_i : E \to E$, $1 \leqslant i \leqslant 3$, definite astfel:

$$f_1(x) = x,\ f_2(x) = (x + \sqrt{3})/(1 - x\sqrt{3}),\ f_3(x) = (x - \sqrt{3})/(1 + x\sqrt{3}),\ \forall\, x \in E.$$

Arătați că $H = \{f_1, f_2, f_3\}$ este stabilă în raport cu operația de compunere a funcțiilor și alcătuiți tabla operației induse.

7. Pe $\mathbf{R}$ definim legea de compoziție $\mathbf{R} \times \mathbf{R} \to \mathbf{R}$, $(x, y) \to x * y$, unde $x * y \overset{\text{def}}{=\!=} x + y + xy$. Arătați că această lege de compoziție este asociativă, comutativă și cu element neutru. Intervalul $[-1, \infty)$ este o parte stabilă a lui $\mathbf{R}$ în raport cu legea de compoziție „$*$".

8. Arătați că legile de compoziție de la ex. 3 sînt asociative și comutative. Studiați existența elementului neutru pentru operațiile induse pe intervalele $[a, b]$, $[a, b)$, $(a, b]$, (a, b) unde $a, b \in \mathbf{R}$, $a < b$.

9. Arătaţi că legile de compoziţie definite pe **N** la ex. 4 sînt asociative şi comutative. Studiaţi existenţa elementului neutru pentru aceste legi de compoziţie şi pentru operaţiile induse pe $H = \{a \in \mathbf{N} \mid a \mid 12\}$.

10. Fie $M = \mathbf{N} \times \mathbf{N}$. Pe mulţimea M introducem legile de compoziţie :

$$(x, y) + (z, w) \overset{\text{def}}{=} (x + z, y + w),$$

$$(x, y)(z, w) \overset{\text{def}}{=} (xz + yw, xw + yz)$$

oricare ar fi perechile (x, y) şi (z, w) din M. Arătaţi că aceste legi de compoziţie sînt asociative, comutative şi cu element neutru.

11. Fie $M = \mathbf{Z} \times \mathbf{Z}^*$, unde $\mathbf{Z}^* = \mathbf{Z} \setminus \{0\}$. Pe mulţimea M introducem următoarele legi de compoziţie :

$$(x, y) + (z, w) \overset{\text{def}}{=} (xw + yz, yw),$$

$$(x, y)(z, w) \overset{\text{def}}{=} (xz, yw)$$

oricare ar fi perechile (x, y) şi (z, w) din M. Arătaţi că aceste legi de compoziţie sînt asociative, comutative şi cu element neutru.

12. Fie $a, b, c \in \mathbf{Z}$, $b \neq 0$. Pe **Z** definim legea de compoziţie „$*$".

$$x*y \overset{\text{def}}{=} axy + b(x + y) + c, \ \forall \ x, y \in \mathbf{Z}.$$

1) Arătaţi că „$*$" este lege de compoziţie asociativă dacă şi numai dacă

$$b^2 - b - ac = 0.$$

2) Cînd $b^2 - b - ac = 0$ legea de compoziţie „$*$" are element neutru dacă şi numai dacă $b \mid c$.

13. Pe mulţimea **N** a numerelor naturale definim legea de compoziţie „$*$",

$$\mathbf{N} \times \mathbf{N} \to \mathbf{N} \ (m, n) \to m*n \overset{\text{def}}{=} m^n.$$

1) Cercetaţi proprietăţile acestei legi de compoziţie.
2) Determinaţi tripletele (m, n, p) de numere naturale diferite de 0 astfel încît

$$(m*n)*p = m*(n*p).$$

14. Pe **R** se defineşte legea de compoziţie „$*$",

$$\mathbf{R} \times \mathbf{R} \to \mathbf{R}, \ (x, y) \to x*y \overset{\text{def}}{=} xy + 2ax + by.$$

Determinaţi a şi b astfel încît legea de compoziţie „$*$" să fie comutativă şi asociativă.

15. Pe **R** se defineşte legea de compoziţie „$*$",

$$\mathbf{R} \times \mathbf{R} \to \mathbf{R} \ (x, y) \to x*y \overset{\text{def}}{=} xy - x - y + 2.$$

Cercetaţi existenţa elementului neutru.

16. Fie M mulţimea matricelor $A \in M_2(\mathbf{R})$,

$$A = \begin{pmatrix} 0 & a \\ 0 & b \end{pmatrix}, \ a, b \in \mathbf{R}$$

Arătaţi :

1) $A, B \in M \Rightarrow AB \in M$;
2) Nu există $U \in M$ astfel încît $UA = A$, $\forall A \in M$;
3) Există o infinitate de matrice $V \in M$ astfel încît $AV = A$, $\forall A \in M$.

Admite element neutru operaţia indusă pe M de înmulţirea matricelor ?

17. Pe $\mathbf{R}_+^* = \{a \in \mathbf{R} \mid a > 0\}$ definim legile de compoziţie :

$$a \perp b \overset{\text{def}}{=} \frac{a+b}{2} \quad \text{(media aritmetică)}$$

$$a \top b \overset{\text{def}}{=} \sqrt{ab} \quad \text{(media geometrică)}$$

$$a \Delta b \overset{\text{def}}{=} \frac{2ab}{a+b} \quad \text{(media armonică)}$$

$$\forall\, a,\ b \in \mathbf{R}_+^*.$$

Arătaţi că aceste legi de compoziţie sînt comutative şi nu sînt asociative. Admit element neutru ?

18. Pe $M_2(\mathbf{R})$ se defineşte legea de compoziţie „*"

$$A * B \overset{\text{def}}{=} AB + BA, \qquad \forall A,\ B \in M_2(\mathbf{R}).$$

Studiaţi dacă legea de compoziţie „*" este asociativă (comutativă). Admite element neutru ?

19. Determinaţi părţile stabile finite ale lui $\mathbf{Z}$ în raport cu înmulţirea. Este $\mathbf{R} \setminus \mathbf{Q}$ parte stabilă a lui $\mathbf{R}$ în raport cu adunarea şi (înmulţirea) ?

20. Fie H mulţimea numerelor reale de forma $a + b\sqrt{2}$, $a,\ b \in \mathbf{Q}$ ce satisfac condiţia $a^2 - 2b^2 = 1$. Arătaţi că H este o parte stabilă a lui $\mathbf{R}$ în raport cu înmulţirea şi că toate numerele din H sînt simetrizabile în raport cu operaţia indusă.

21. Fie M mulţimea matricelor $A \in M_2(\mathbf{R})$,

$$A = \begin{pmatrix} a & 0 \\ c & b \end{pmatrix},\ a,\ b,\ c \in \mathbf{R}.$$

1) Dacă $A,\ B \in M$, atunci $AB \in M$.

2) Care sînt elementele simetrizabile ale lui M în raport cu operaţia indusă ?

22. Determinaţi elementele simetrizabile în raport cu înmulţirea modulo 12 din $\mathcal{R}_{12}$.

23. Examinînd tabla înmulţirii modulo 8, deduceţi că pentru ecuaţia $a \otimes x \oplus b = 0$, cu $a,\ b \in \mathcal{R}_8$, $a \neq 0$, sînt posibile numai cazurile :

1) nu are nici o soluţie în $\mathcal{R}_8$;

2) are o singură soluţie în $\mathcal{R}_8$;

3) are două soluţii în $\mathcal{R}_8$;

4) are patru soluţii în $\mathcal{R}_8$.

Daţi cîte un exemplu de astfel de ecuaţie pentru fiecare tip.

24. Găsiţi toate soluţiile din $\mathcal{R}_{12}$ ale sistemului de ecuaţii liniare

$$\begin{cases} 3 \otimes x \oplus 4 \otimes y = 11, \\ 4 \otimes x \oplus 9 \otimes y = 10. \end{cases}$$

* * *

25. Fie $n > 0$ un număr întreg şi

$$M = \{(a,\ b) \mid a,\ b \in \mathbf{Z},\ (a,\ n) = 1\}.$$

1) Dacă $(a,\ b),\ (c,\ d) \in M \Rightarrow (ac,\ ad + bc) \in M$;

2) Legea de compoziţie „*" definită prin M prin :

$$(a,\ b) * (c,\ d) = (ac,\ ad + bc)$$

este comutativă şi asociativă.

3) Determinaţi elementul neutru şi elementele simetrizabile.

26*. Pe o mulţime M se dă o lege de compoziţie asociativă

$$M \times M \to M, \ (x, y) \to xy.$$

Presupunem că $\exists a \in M$ astfel încît $y \in aMa = \{axa \mid x \in M\}, \ \forall y \in M$.
Arătaţi că o asemenea lege de compoziţie admite element neutru.

27*. Fie „$\top$" şi „$\perp$" două legi de compoziţie pe mulţimea M, cu elemente neutre e respectiv e'. Dacă oricare ar fi $x, y, u, v \in M$ avem :

$$(x \top y) \perp (u \top v) = (x \perp u) \top (y \perp v),$$

atunci :

1) $e = e'$,
2) $x \top y = x \perp y, \qquad \forall x, y \in M$.
3) $x \perp y = y \perp x, \qquad \forall x, y \in M$.

28*. Fie M o mulţime cu trei elemente.

1) Cîte legi de compoziţie se pot defini pe M ?
2) Cîte dintre acestea sînt comutative ?
3) Cîte admit element neutru ?

Generalizare.

29*. Pe mulţimea punctelor unui plan Π definim legea de compoziţie $\varphi : \Pi \times \Pi \to \Pi$ $\varphi(A, B) \overset{\text{def}}{=} C \Leftrightarrow C$ este simetricul lui A în raport cu B.

1) Arătaţi că φ nu este asociativă şi nici comutativă.

2) Raportînd punctele planului la un reper x_1Ox_2, arătaţi că mulţimea H a punctelor planului de coordonate întregi este inclusă în orice parte stabilă T a lui Π în raport cu φ care conţine punctele de coordonate (0, 0), (1, 0), (0, 1), (1, 1).

30*. Fie M mulţimea tuturor secvenţelor de opt litere din alfabetul latin, numite *cuvinte* de lungime 8 peste alfabetul latin. Dacă $\alpha, \beta \in M$, definim cuvintele $\alpha * \beta$ şi $\alpha \circ \beta$ astfel : $\alpha * \beta$ este cuvîntul format cu primele 5 litere ale lui α urmate de ultimele trei litere ale lui β, iar $\alpha \circ \beta$ este cuvîntul format din ultimele 4 litere ale lui α urmate de primele patru litere ale lui β. Astfel, dacă α = aartbbcd şi β = csttrabb, atunci $\alpha * \beta$ = aartbabb şi $\alpha \circ \beta$ = = bbcdcstt. Arătaţi că legea de compoziţie „$*$" este asociativă, iar „$\circ$" nu este asociativă. Studiaţi comutativitatea.

§ 1. MONOIZI

Algebra modernă are ca subiect studiul structurilor algebrice. Prin *structură algebrică* se înțelege o mulțime nevidă M înzestrată cu una sau mai multe legi de compoziție φ, ψ, ..., care satisfac o listă specifică de proprietăți, numite *axiomele* structurii.

Prima structură algebrică pe care o introducem este structura de monoid. Prin *monoid* se înțelege un cuplu (M, φ) format cu o mulțime nevidă M și o lege de compoziție definită pe M, $\varphi : M \times M \to M$, asociativă și cu element neutru. Se mai spune că M este (formează) monoid în raport cu operația φ.

Mai sistematic, folosind de exemplu notația „$*$" pentru legea de compoziție, definiția monoidului se poate da astfel :

1.1. *Definiție.* **O mulțime nevidă M este monoid în raport cu o lege de compoziție definită pe M,**

$$M \times M \to M, \ (x, y) \to x*y$$

dacă sînt satisfăcute următoarele axiome :

$M_1)$ $\quad (x*y)*z = x*(y*z), \quad \forall x, y, z \in M$;

$M_2)$ $\quad \exists\, e \in M$ **astfel încît** $e*x = x*e = x, \quad \forall x \in M$.

Dacă pentru legea de compoziție φ a monoidului se folosește una din notațiile „$*$", „$+$", „$\cdot$" etc. atunci în loc de (M, φ) scriem $(M, *)$, $(M, +)$, $(M, \cdot)$ etc.

Adesea cuplul (M, φ) se notează tot cu M ; în acest caz M se interpretează fie ca fiind cuplul (M, φ), fie ca fiind mulțimea *suport* (*subiacentă*) a structurii de monoid.

Ansamblul de condiții M_1, M_2 poartă numele de *axiomele monoidului*. Elementul $e \in M$ care satisface axioma M_2 este unic determinat (v. Teorema 6.2, Cap. II) și se numește *elementul neutru* al monoidului M.

Vom nota cu $U(M)$ mulțimea elementelor lui M simetrizabile în raport cu operația acestuia. Cînd M este dat în notație multiplicativă, elementele din $U(M)$ se mai numesc încă și *unități* ale monoidului M.

Spunem că monoidul M este *comutativ* dacă operația acestuia satisface și axioma :

$M_3)$ $\quad x*y = y*x, \quad \forall x, y \in M$.

Exemple

1. Adunarea numerelor este asociativă, comutativă şi admite pe 0 ca element neutru. Rezultă că $(\mathbf{N}, +)$ este monoid comutativ, numit *monoidul aditiv* al numerelor naturale. De asemenea, $(\mathbf{N}, \cdot)$ este monoid comutativ, numit *monoidul multiplicativ* al numerelor naturale.

2. Fie E o mulţime şi $\mathfrak{P}(E)$ mulţimea tuturor părţilor lui E.
Cum:

$$\begin{array}{lll} M_1) & (X \cup Y) \cup Z = X \cup (Y \cup Z), & \forall X, Y, Z \in \mathfrak{P}(E) \\ M_2) & \varnothing \cup X = X \cup \varnothing = X, & \forall X \in \mathfrak{P}(E) \\ M_3) & X \cup Y = Y \cup X, & \forall X, Y, Z \in \mathfrak{P}(E) \end{array}$$

rezultă că $(\mathfrak{P}(E), \cup)$ este monoid comutativ.

Analog, $(\mathfrak{P}(E), \cap)$ este monoid comutativ.

3. Fie E o mulţime şi $\mathfrak{F}(E)$ mulţimea tuturor funcţiilor $f: E \to E$. Cum

$$\begin{array}{lll} M_1) & (f \circ g) \circ h = f \circ (g \circ h), & \forall f, g, h \in \mathfrak{F}(E) \\ M_2) & 1_E \circ f = f \circ 1_E = f, & \forall f \in \mathfrak{F}(E) \end{array}$$

rezultă că $\mathfrak{F}(E)$ formează monoid în raport cu operaţia de compunere. Dacă E are cel puţin două elemente, atunci $(\mathfrak{F}(E), \circ)$ nu este monoid comutativ (v. tabla operaţiei lui $\mathfrak{F}(E)$ cînd $E = \{1, 2\}$; Cap. II, § 3).

Să observăm că într-un monoid M sînt adevărate toate rezultatele obţinute în Cap. II în legătură cu elementele simetrizabile.

Dacă $a \in M$ definim inductiv *puterile* lui a cu exponenţi numere naturale astfel:

$$a^0 = e, \quad a^1 = a, \quad a^2 = aa, \quad a^3 = a^2 a, \quad \ldots, \quad a^n = a^{n-1}a, \quad \ldots$$

sau mai condensat prin

$$a^n \overset{\text{def}}{=} \begin{cases} e & \text{dacă } n = 0, \\ a^{n-1} \cdot a & \text{dacă } n > 0. \end{cases}$$

1.2. Teoremă. Oricare ar fi numerele naturale m şi n avem:

$$\boxed{a^m \cdot a^n = a^{m+n}, \quad (a^m)^n = a^{mn}}$$

Demonstraţie. Este suficient să arătăm că pentru m fixat, afirmaţiile din enunţ sînt adevărate oricare ar fi $n \in \mathbf{N}$. Cum

$$a^m \cdot a^0 = a^m \cdot e = a^m = a^{m+0}$$

şi

$$(a^m)^0 = e = a^0 = a^{m \cdot 0},$$

afirmaţiile din enunţ sînt adevărate pentru $n = 0$.

Presupunem că $n > 0$ şi că afirmaţiile din enunţ sînt adevărate pentru $n-1$. Atunci:

$$a^m a^n = a^m(a^{n-1}\cdot a) = (a^m\cdot a^{n-1})a = a^{m+n-1}a = a^{m+n}$$

şi

$$(a^m)^n = (a^m)^{n-1}\cdot a^m = a^{m(n-1)}\cdot a^m = a^{m(n-1)+m} = a^{mn}.$$

Analog, dacă legea de compoziţie a monoidului M este dată aditiv, definim *multiplii* na ai lui a, cu $n \in \mathbf{N}$, astfel:

$$na \stackrel{\text{def}}{=} \begin{cases} 0 & \text{dacă } n = 0 \\ (n-1)a + a & \text{dacă } n > 0. \end{cases}$$

Rezultatul din teorema precedentă se transcrie aditiv astfel:

$$ma + na = (m+n)a, \quad n(ma) = (nm)a \quad \forall m, n \in \mathbf{N}$$

Exerciţii rezolvate

R — 1 Fie M mulţimea tuturor matricelor $A \in M_2(\mathbf{Z})$ de forma:

$$A = \begin{pmatrix} a & c \\ 0 & b \end{pmatrix}, \quad a, b, c \in \mathbf{Z}.$$

1) Să se arate că M este o parte stabilă a lui $M_2(\mathbf{Z})$ în raport cu înmulţirea matricelor şi că formează monoid în raport cu operaţia indusă.

2) Determinaţi elementele simetrizabile ale monoidului M.

Soluţie. 1) Fie $A, B \in M_2(\mathbf{Z})$.

$$A = \begin{pmatrix} a & c \\ 0 & b \end{pmatrix}, \quad B = \begin{pmatrix} u & w \\ 0 & v \end{pmatrix}.$$

Avem:

$$AB = \begin{pmatrix} a & c \\ 0 & b \end{pmatrix}\begin{pmatrix} u & w \\ 0 & v \end{pmatrix} = \begin{pmatrix} au & aw + cv \\ 0 & bv \end{pmatrix} \in M.$$

Rezultă că M este o parte stabilă a lui $M_2(\mathbf{Z})$ în raport cu înmulţirea matricelor. Cum

$$E = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \in M$$

rezultă că operaţia indusă pe M admite element neutru, anume pe E. Operaţia indusă este şi asociativă căci înmulţirea matricelor este asociativă. Rezultă că $(M, \cdot)$ este monoid.

2) Presupunem că $A \in U(M)$. Atunci există $B \in M$ astfel încît $AB = BA = E$. Cum

$$1 = \det(E) = \det(AB) = \det(A)\det(B)$$

şi $\det(A)$, $\det(B)$ sînt numere întregi, rezultă că $\det(A) = \pm 1$, deci

$$ab = \begin{vmatrix} a & c \\ 0 & b \end{vmatrix} = \pm 1.$$

Cum a, $b \in \mathbb{Z}$ rezultă că $ab = 1$ dacă $a = 1$, $b = 1$ sau $a = -1$, $b = -1$ şi $ab = -1$ dacă $a = -1$, $b = 1$ sau $a = 1$, $b = -1$. Aşadar, dacă $A \in U(M)$ atunci A este egală cu una din matricele :

$$\begin{pmatrix} 1 & c \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} -1 & c \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} -1 & c \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & c \\ 0 & -1 \end{pmatrix}, \ c \in \mathbb{Z}.$$

Reciproc, matricele din lista precedentă sînt elemente inversabile ale monoidului M, inversele lor fiind respectiv matricele :

$$\begin{pmatrix} 1 & -c \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} -1 & -c \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} -1 & c \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & c \\ 0 & -1 \end{pmatrix}, \ c \in \mathbb{Z}$$

după cum uşor se poate verifica.

R — 2 Fie E o mulţime nevidă şi $f \in \mathcal{F}(E)$. Următoarele afirmaţii sînt echivalente :

a) f este element simetrizabil al monoidului $(\mathcal{F}(E), \circ)$;

b) f este funcţie bijectivă.

Enumeraţi elementele simetrizabile ale monoidului $(\mathcal{F}(E), \circ)$, unde $E = \{1, 2, 3\}$.

Soluţie. a) $\Rightarrow$ b). Cum f este element simetrizabil, există $g \in \mathcal{F}(E)$ astfel încît :

$$f \circ g = g \circ f = 1_E.$$

Rezultă că f este funcţie bijectivă (v. Ex. **R — 1**, Cap. I).

b) $\Rightarrow$ a). Cum $f : E \to E$ este funcţie bijectivă, pentru orice $y \in E$ există $x \in E$ unic determinat astfel încît $y = f(x)$. Definim $g : E \to E$ prin :

$$g(y) \overset{\text{def}}{=\!=} x \Leftrightarrow f(x) = y, \quad \forall\, y \in E.$$

Avem :

$$(f \circ g)(y) = f(g(y)) = f(x) = y = 1_E(y), \quad \forall\, y \in E$$

şi

$$(g \circ f)(x) = g(f(x)) = g(y) = x = 1_E(x), \quad \forall\, x \in E,$$

de unde

$$f \circ g = g \circ f = 1_E$$

deci f este element simetrizabil al monoidului $(\mathcal{F}(E), \circ)$.

Presupunem că $E = \{1, 2, 3\}$ şi $f \in \mathcal{F}(E)$. Cu convenţia de la § 3, cap. II, funcţia f se poate da prin :

$$f = \begin{pmatrix} 1 & 2 & 3 \\ f(1) & f(2) & f(3) \end{pmatrix}.$$

Evident, $\mathcal{F}(E)$ are $3 \times 3 \times 3 = 27$ elemente, f fiind simetrizabil ($\equiv$ bijectiv) dacă şi numai dacă valorile sale $f(1)$, $f(2)$, $f(3)$ reproduc, într-o ordine arbitrară, numerele 1, 2, 3. Avem deci $3! = 6$ elemente simetrizabile, anume :

$$e = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \quad \sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \quad \pi = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

$$\alpha = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \quad \beta = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \quad \gamma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

Aşadar $U(\mathcal{F}(E)) = \{e, \sigma, \pi, \alpha, \beta, \gamma\}$.

§ 2. DEFINIŢIA GRUPULUI. EXEMPLE

Noţiunea de grup ocupă un loc central printre structurile algebrice. Teoria grupurilor are în esenţă o sursă unică : *studiul, în raport cu operaţia de compunere, al funcţiilor bijective ale unei mulţimi în ea însăşi*.

Definiţia noţiunii de *grup* se dă imediat cu ajutorul celei de monoid : un monoid G cu proprietatea că orice element $x \in G$ este simetrizabil (în raport cu operaţia acestuia) se numeşte *grup*. Mai precis :

2.1. *Definiţie.* Un cuplu $(G, *)$ format cu o mulţime nevidă G şi cu o lege de compoziţie pe G,

$$G \times G \to G, \ (x, y) \to x*y$$

se numeşte *grup* dacă sînt satisfăcute următoarele axiome :

$G_1)$ $\quad (x*y)*z = x*(y*z), \quad \forall\ x, y, z \in G$;

$G_2)$ $\quad \exists\ e \in G$ **astfel încît** $e*x = x*e = x, \ \forall\ x \in G$;

$G_3)$ $\quad \forall\ x \in G, \exists x' \in G$ **astfel încît** $x'*x = x*x' = e$.

Elementul $e \in G$, a cărui existenţă este asigurată de axioma G_2, este unic determinat (v. Teorema 6.2, Cap. I) şi se numeşte *elementul neutru* al grupului G. Elementul x' a cărui existenţă este asigurată de axioma G_3 pentru orice $x \in G$, este unic determinat (v. § 7, Cap. II) şi se numeşte *simetricul* lui x ; în notaţia multiplicativă punem $x' = x^{-1}$, iar în notaţia aditivă punem $x' = -x$, numit *inversul*, respectiv *opusul* lui x.

Ansamblul de condiţii G_1, G_2 şi G_3 poartă numele de *axiomele grupului*. Dacă în plus este satisfăcută şi axioma :

$$G_4) \quad x*y = y*x, \quad \forall\ x, y \in G,$$

atunci cuplul $(G, *)$ se numeşte *grup comutativ* sau *grup abelian*.

Exemple

1. *Grupul permutărilor.* Fie $E = \{1, 2, 3\}$.

Să notăm cu $\mathfrak{S}_3$ mulţimea tuturor funcţiilor bijective de la E la E. Folosind convenţia de la § 3, Cap. II, acestea pot fi descrise astfel :

$$1_E = e = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \quad \sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \quad \pi = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

$$\alpha = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \quad \beta = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \quad \gamma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

deci $\mathfrak{S}_3 = \{e, \sigma, \pi, \alpha, \beta, \gamma\}$.

Cum compusa a două funcţii bijective este o funcţie bijectivă (v. Teorema 2.2, Cap. 1) rezultă că $\mathfrak{S}_3$ este o parte stabilă a lui $\mathcal{F}(E)$ în raport cu compunerea funcţiilor.

Să alcătuim tabla operaţiei induse pe $\mathfrak{S}_3$ de către compunerea funcţiilor, operaţie numită *compunerea permutărilor* de trei obiecte.

$\circ$	e	σ	π	α	β	γ
e	e	σ	π	α	β	γ
σ	σ	π	e	γ	α	β
π	π	e	σ	β	γ	α
α	α	β	γ	e	σ	π
β	β	γ	α	π	e	σ
γ	γ	α	β	σ	π	e

Tabla grupului $\mathfrak{S}_3$.

Avem, de exemplu, $\sigma\circ\alpha = \gamma$. În adevăr,

$$(\sigma\circ\alpha)\ (1) = \sigma(\alpha(1)) = \sigma(1) = 2 = \gamma(1),$$

$$(\sigma\circ\alpha)\ (2) = \sigma(\alpha(2)) = \sigma(3) = 1 = \gamma(2),$$

$$(\sigma\circ\alpha)\ (3) = \sigma(\alpha(3)) = \alpha(2) = 3 = \gamma(3)$$

de unde $\sigma\circ\alpha = \gamma$.

Cum compunerea funcţiilor este asociativă şi $1_E = e \in \mathfrak{S}_3$, rezultă că $(\mathfrak{S}_3, \circ)$ este monoid. Se observă pe tabla operaţiei lui $\mathfrak{S}_3$ că orice element din $\mathfrak{S}_3$ este simetrizabil, anume:

$$e^{-1} = e,\ \sigma^{-1} = \pi,\ \pi^{-1} = \sigma,\ \alpha^{-1} = \alpha,\ \beta^{-1} = \beta,\ \gamma^{-1} = \gamma.$$

Rezultă că $(\mathfrak{S}_3, \circ)$ este grup, numit *grupul permutărilor* de trei obiecte sau încă *grupul simetric* de grad 3. Din tabla operaţiei lui $\mathfrak{S}_3$ rezultă că acesta nu este grup comutativ.

Analog, dacă $n>1$ şi $E=\{1, 2, \ldots, n\}$ atunci mulţimea $\mathfrak{S}_n$ a funcţiilor bijective de la E la E formează grup în raport cu operaţia de compunere a funcţiilor ; $(\mathfrak{S}_n, \circ)$ se numeşte *grupul permutărilor* de n obiecte sau *grupul simetric* de grad n.

2. *Grupul lui Klein*. Fie $E = \mathbf{R} \times \mathbf{R}$ şi $\mathcal{K} = \{1_E, u, v, w\}$, unde u, v şi w sînt următoarele funcţii de la E la E (v. fig. III.1) ;

$$u : E \to E, \qquad u(x) = (x_1, -x_2),$$

$$v : E \to E, \qquad v(x) = (-x_1, x_2),$$

$$w : E \to E, \qquad w(x) = (-x_1, -x_2),$$

oricare ar fi $x = (x_1, x_2) \in E = \mathbf{R} \times \mathbf{R}$.

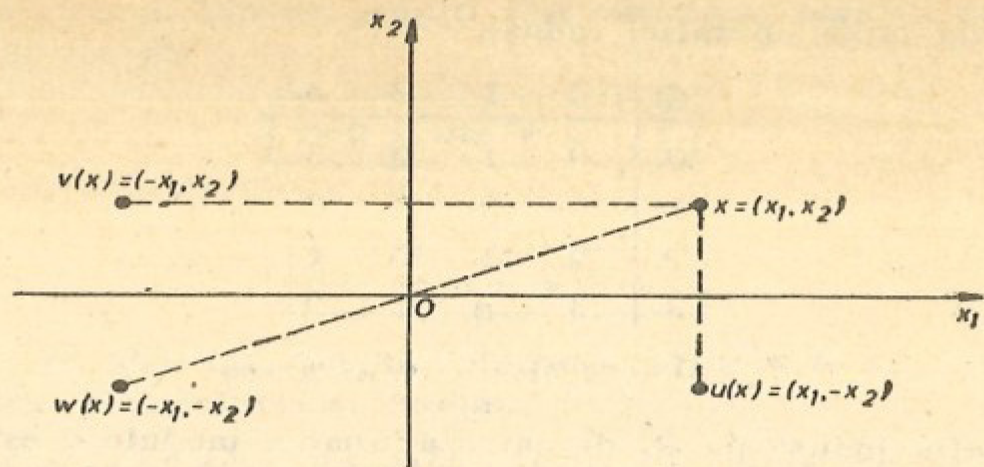


Fig. III.1.

Dacă compunem două funcții din $\mathcal{K}$ se obține tot o funcție din $\mathcal{K}$. De exemplu, avem $u \circ v = w$. În adevăr, pentru orice $x \in E$, $x = (x_1, x_2)$, avem :

$$(u \circ v)(x) = u(v(x)) = u((-x_1, x_2)) = (-x_1, -x_2) = w(x),$$

de unde $u \circ v = w$. Să alcătuim tabla operației indusă pe $\mathcal{K}$ de către compunerea funcțiilor din $\mathcal{F}(E)$.

$\circ$	1_E	u	v	w
1_E	1_E	u	v	w
u	u	1_E	w	v
v	v	w	1_E	u
w	w	v	u	1_E

Tabla grupului Klein.

Cum compunerea funcțiilor este asociativă și $1_E \in \mathcal{K}$, rezultă că $(\mathcal{K}, \circ)$ este monoid. Se observă pe tabla operației lui $\mathcal{K}$ că orice element din $\mathcal{K}$ este simetrizabil, anume :

$$1_E^{-1} = 1_E, \ u^{-1} = u, \ v^{-1} = v, \ w^{-1} = w.$$

Așadar $(\mathcal{K}, \circ)$ este grup, numit *grupul lui Klein*. Din tabla operației, se deduce că grupul lui Klein este comutativ. Să observăm că elementele grupului $\mathcal{K}$ sînt funcții bijective. Aceasta se poate verifica direct sau observînd că $u \circ u = 1_E$, $v \circ v = 1_E$, $w \circ w = 1_E$ și aplicînd apoi rezultatul de la Ex. R—1, Cap. I.

3. *Grupul* $(\mathcal{R}_n, \oplus)$ *al resturilor modulo n*. Fie $n = 4$ și $\mathcal{R}_4 = \{0, 1, 2, 3\}$. Se știe că $\mathcal{R}_4$ este o parte stabilă a lui $\mathbb{Z}$ în raport cu adunarea modulo 4.

Să alcătuim tabla operației induse.

$\oplus$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

Tabla grupului $(\mathcal{R}_4, \oplus)$.

Operația indusă pe $\mathcal{R}_4$ de către adunarea modulo 4 este asociativă (v. § 8, Cap. II). Din tabla acestei operații rezultă că admite pe 0 ca element neutru, că este comutativă și că orice element din $\mathcal{R}_4$ este simetrizabil în raport cu operația indusă :

$$-0 = 0, \ -1 = 3, \ -2 = 2, \ -3 = 1.$$

Așadar, $(\mathcal{R}_4, \oplus)$ este grup abelian. Analog se arată că $(\mathcal{R}_n, \oplus)$ este grup abelian, unde $\mathcal{R}_n = \{0, 1, 2, \ldots, n-1\}$ iar „$\oplus$" este operația indusă pe $\mathcal{R}_n$ de către adunarea modulo n, numit *grupul resturilor modulo n*.

4. Din proprietățile adunării și înmulțirii numerelor, menționate în Cap. 1, § 1, rezultă că

$$(\mathbf{Z}, +), (\mathbf{Q}, +), (\mathbf{R}, +) \text{ și } (\mathbf{C}, +)$$

sînt grupuri abeliene, numite respectiv *grupul aditiv* al numerelor întregi, raționale, reale, complexe.

De asemenea, notînd

$$\mathbf{Q}^* = \mathbf{Q} \setminus \{0\}, \ \mathbf{R}^* = \mathbf{R} \setminus \{0\} \text{ și } \mathbf{C}^* = \mathbf{C} \setminus \{0\},$$

atunci

$$(\mathbf{Q}^*, \cdot), (\mathbf{R}^*, \cdot) \text{ și } (\mathbf{C}^*, \cdot)$$

sînt grupuri *abeliene*, numite respectiv *grupul multiplicativ* al numerelor raționale, reale, complexe diferite de zero.

§ 3. REGULI DE CALCUL ÎNTR-UN GRUP

Cum orice grup este monoid, calculul algebric cu elementele unui grup beneficiază de toate regulile valabile pentru legile de compoziție asociative și cu element neutru (v. § 1).

Pe de altă parte, pentru grupuri avem o serie de reguli care nu sînt întotdeauna aplicabile în cazul monoizilor. În esență, aceste reguli se fundamentează pe proprietatea că orice element al unui grup este simetrizabil în raport cu operația acestuia.

3.1. Teoremă. Într-un grup G sînt adevărate regulile de simplificare la stînga şi la dreapta :

$$\boxed{a*b = a*c \Rightarrow b = c},$$

respectiv

$$\boxed{b*a = c*a \Rightarrow b = c}.$$

Demonstraţie. Presupunem că pentru $a, b, c \in G$ avem $a*b = a*c$ şi fie a' simetricul elementului a. Avem :

$$b = e*b = (a'*a)*b = a'*(a*b) = a'*(a*c) = (a'*a)*c = e*c = c,$$

deci $b = c$, de unde rezultă că este adevărată regula de simplificare la stînga. Analog se demonstrează regula de simplificare la dreapta.

3.2. Teoremă. Fie $(G, *)$ un grup. Oricare ar fi $a, b \in G$, ecuaţiile :

$$a*x = b \text{ şi } y*a = b$$

au soluţii unice în G, anume $x = a'*b$, respectiv $y = b*a'$, unde a' este simetricul lui a.

Demonstraţie. Dacă x_1 şi x_2 sînt soluţii din G ale ecuaţiei $a*x = b$, atunci

$$a*x_1 = b = a*x_2,$$

deci $a*x_1 = a*x_2$ şi folosind regula de simplificare la stînga obţinem $x_1 = x_2$. Aşadar, ecuaţia $a*x = b$ are cel mult o soluţie în G.

Fie $x = a'*b$, unde a' este simetricul lui a.

Avem :

$$a*x = a*(a'*b) = (a*a')*b = e*b = b,$$

de unde rezultă că $x = a'*b$ este soluţie (din G) a ecuaţiei $a*x = b$, unică conform primei părţi a demonstraţiei. Analog se arată că ecuaţia $y*a = b$ admite soluţie unică, $y = b*a'$.

Dacă grupul G este dat în notaţia aditivă (multiplicativă) atunci rezultatele din teoremele precedente se transcriu astfel :

$$a + b = a + c \text{ sau } b + a = c + a \Rightarrow b = c,$$

$$a + x = b \Rightarrow x = (-a) + b,$$

$$y + a = b \Rightarrow y = b + (-a) = b - a,$$

respectiv

$$ab = ac \text{ sau } ba = ca \Rightarrow b = c,$$

$$ax = b \Rightarrow x = a^{-1}b,$$

$$ya = b \Rightarrow y = ba^{-1}.$$

Cum operația unui grup este asociativă și cu element neutru, toate rezultatele din § 1 sînt adevărate și în cazul grupurilor. Astfel, dacă G este grup multiplicativ, $a \in G$ și $n \in \mathbf{N}$, atunci punînd

$$a^n = \begin{cases} e & \text{dacă } n = 0 \\ a^{n-1}a & \text{dacă } n > 0 \end{cases}$$

avem :

$$a^m a^n = a^{m+n},\ (a^m)^n = a^{mn},\ \forall\ m,\ n \in \mathbf{N}.$$

Pentru elementele unui grup putem defini și puteri ale acestora cu exponenți numere întregi negative, după cum urmează.

Dacă $a \in G$ și $n \in \mathbf{Z}$, $n < 0$, atunci $-n > 0$, deci are sens a^{-n} precum și inversul acestuia, anume $(a^{-n})^{-1}$. Punem deci :

$$a^n \stackrel{\text{def}}{=} (a^{-n})^{-1}, \qquad \forall\ n \in \mathbf{Z},\ n < 0$$

și avem :

$$\boxed{a^m a^n = a^{m+n}, \quad (a^m)^n = a^{mn}, \quad \forall\ m,\ n \in \mathbf{Z}}$$

O cale de demonstrație a acestei afirmații este reducerea la cazul exponenților nenegativi, care a fost deja demonstrat (v. § 1).

Astfel, dacă $m < 0$ și $n < 0$ avem :

$$a^m a^n = (a^{-m})^{-1}(a^{-n})^{-1} = (a^{-n} \cdot a^{-m})^{-1} = (a^{(-n)+(-m)})^{-1} = (a^{-(m+n)})^{-1} = a^{m+n}.$$

Presupunem că $m > 0$, $n < 0$. Dacă $m \geqslant |\, n \,|$ există $r \geqslant 0$ astfel încît $m = -n + r$ și atunci

$$a^m a^n = a^{r+(-n)}a^n = a^r a^{-n}(a^{-n})^{-1} = a^r = a^{m+n}$$

ș.a.m.d.

Dacă grupul G este dat în notație aditivă, atunci cele de mai sus devin proprietăți pentru *multiplii întregi* ai elementelor lui G :

$$\boxed{ma + na = (m + n)a,\ n(ma) = (nm)a,\ \forall\ m,\ n \in \mathbf{Z}}$$

Cum pentru orice $a \in G$ și $n \in \mathbf{Z}$ avem

$$a^n a^{-n} = a^{n+(-n)} = a^0 = e = a^{(-n)}a^n$$

rezultă că :

$$\boxed{(a^n)^{-1} = a^{-n},\ \forall\ a \in G,\ n \in \mathbf{Z}}$$

Analog, în notație aditivă avem :

$$\boxed{-(na) = (-n)a,\ \forall\ a \in G,\ n \in \mathbf{Z}}$$

Exerciții rezolvate

R — 1 Fie $\varepsilon = -\frac{1}{2} + \frac{i\sqrt{3}}{2} \in \mathbf{C}$. Arătați că

$$\varepsilon^{n^3-n+1} = \varepsilon, \ \forall\, n \in \mathbf{Z}.$$

Soluție. Cum $\varepsilon = \cos\frac{2\pi}{3} + i\sin\frac{2\pi}{3}$, avem :

$$\varepsilon^3 = \cos 2\pi + i\sin 2\pi = 1.$$

Observînd că $n^3 - n = (n-1)n(n+1)$, rezultă că $n^3 - n$ se divide cu 3, deci $n^3 - n = 3q$, cu $q \in \mathbf{Z}$. Dar ε este element al grupului $(C^*, \cdot)$ și folosind regulile de calcul cu puterile întregi ale unui element dintr-un grup multiplicativ, avem :

$$\varepsilon^{n^3-n+1} = \varepsilon^{3q+1} = \varepsilon^{3q}\cdot\varepsilon^1 = (\varepsilon^3)^q\varepsilon^1 = 1^q\varepsilon = \varepsilon.$$

R — 2 Arătați că în orice linie (coloană) a tablei operației unui grup G cu un număr finit de elemente, fiecare element al lui G apare o dată și numai o singură dată.

Soluție. Presupunem că operația grupului G este notată multiplicativ și că $G = \{a_1, a_2, \ldots, a_n\}$, cu $a_i \neq a_j$ pentru $i \neq j$. Fie $a \in G$. În linia lui a din tabla operației grupului G apar elementele :

$$aa_1,\ aa_2,\ \ldots,\ aa_i,\ \ldots,\ aa_n.$$

Dacă $i \neq j$, atunci $aa_i \neq aa_j$. În adevăr, dacă $aa_i = aa_j$, prin simplificare cu a se obține $a_i = a_j$. Contradicție. Rezultă că elementele $aa_1, aa_2, \ldots, aa_n$ sînt distincte, și mai puțin ordinea, coincid cu $a_1, a_2, \ldots, a_n$.

R — 3 Fie G un grup multiplicativ cu patru elemente, $G = \{e, a, b, c\}$, unde e este elementul neutru. Alcătuiți tabla operației grupului G dacă se știe că $a^2 = e$ și $c^2 = e$.

Soluție. Cunoscînd că e este element neutru și că $a^2 = c^2 = e$, în tabla operației lui G se pot completa următoarele poziții :

$\cdot$	e	a	b	c
e	e	a	b	c
a	a	e	?	?
b	b	?	?	?
c	c	?	?	e

Ca să nu avem repetiții în linia lui a și în coloana lui b, la intersecția acestora, nu putem pune a, e sau b, deci $ab = c$. Analog se arată apoi succesiv că $ac = b$, $bc = a$, $bb = e$, $ba = c$, $ca = b$, $cb = a$.

$\cdot$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

R — 4 Fie $(G, \cdot)$ un grup cu n elemente și e elementul neutru al lui G.

1) Demonstrați în cazul cînd G este comutativ că

$$a^n = e, \quad \forall a \in G.$$

2) Verificați această proprietate în cazul grupului $\mathfrak{S}_3$.

Soluție. 1) Fie $a_1, a_2, \ldots, a_n$ elementele grupului G și fie a un element arbitrar din G. Conform cu Ex. R—2, elementele

$$aa_1, aa_2, \ldots, aa_n$$

coincid, mai puțin ordinea, cu $a_1, a_2, \ldots, a_n$ și cum G este comutativ avem :

$$a_1a_2 \ldots a_n = aa_1aa_2\ldots aa_n = \underbrace{aa\ldots a}_{n \text{ ori}}a_1a_2\ldots a_n = a^na_1a_2\ldots a_n.$$

Așadar :

$$e(a_1, \cdot a_2, \cdot \ldots, \cdot a_n) = a^n(a_1, \cdot a_2, \cdot \ldots, \cdot a_n)$$

și prin simplificare se obține $e = a^n$.

2) Grupul $\mathfrak{S}_3$ are 6 elemente, deci $n = 6$.

Păstrînd notațiile folosite la § 2, pentru elementele grupului $\mathfrak{S}_3$ și folosind tabla operației grupului $\mathfrak{S}_3$ se obține $\sigma^3 = e$, $\pi^3 = e$, $\alpha^2 = e$, $\beta^2 = e, \gamma^2 = e$. Astfel din tabla operației grupului $\mathfrak{S}_3$ deducem :

$$\sigma^6 = \sigma\circ\sigma = \pi, \quad \sigma^3 = \sigma^2\circ\sigma = \pi\circ\sigma = e.$$

Avem :

$$\sigma^6 = \sigma^{3\times 2} = (\sigma^3)^2 = e^2 = e\,; \quad \alpha^6 = \alpha^{2\times 3} = (\alpha^2)^3 = e^3 = e \text{ etc.}$$

Remarcă. Se poate demonstra că rezultatul de la pct. 1) este adevărat și pentru grupuri necomutative, așa cum de altfel s-a verificat pentru grupul $\mathfrak{S}_3$.

§ 4. SUBGRUP. EXEMPLE

Fizionomia unui grup G se descrie în esență cu ajutorul subgrupurilor sale : submulțimi nevide H ale lui G cărora operația lui G le conferă, de asemenea, o structură de grup.

Mai precis :

4.1. *Definiție.* Fie $(G, *)$ un grup. O submulțime nevidă H a lui G se numește *subgrup* al lui G dacă sînt satisfăcute următoarele condiții :

1) $\forall\, x, y \in H \Rightarrow x*y \in H$;

2) $\forall\, x \in H \Rightarrow x' \in H$,

unde x' este simetricul lui x (în raport cu operația lui G).

Dacă grupul G este dat în notația aditivă, atunci condițiile 1) și 2) din definiția subgrupului se transcriu astfel :

1) $\forall\, x, y \in H \Rightarrow x + y \in H$;

2) $\forall\, x \in H \Rightarrow -x \in H$.

4.2. Teoremă. Fie $(G, *)$ un grup, e elementul neutru al lui G şi H un sugrup al lui G. Atunci:

1) $e \in H$,

2) H este grup în raport cu operaţia indusă pe H de către operaţia grupului G.

Demonstraţie. 1) Cum $H \neq \varnothing$ putem alege un element $x \in H$. Din 2) rezultă că şi $x' \in H$ şi acum din 1) rezultă că $e = x' * x \in H$.

2) Să notăm cu φ operaţia grupului G, $\varphi : G \times G \to G$. Din 1) rezultă că H este o parte stabilă a lui G în raport cu operaţia φ. Fie φ' legea de compoziţie indusă pe H de φ,

$$\varphi' : H \times H \to H, \ (x, y) \to \varphi'(x, y) \overset{\text{def}}{=\!=} \varphi(x, y).$$

Evident φ' este asociativă (căci φ este asociativă) şi admite ca element neutru pe $e \in H$. Dacă $x \in H$, atunci simetricul său x' în raport cu φ se găseşte în H, deci este simetric al lui x şi în raport cu φ'. Rezultă ca (H, φ') este grup.

Exemple

1. Fie $(G, *)$ un grup, e elementul său neutru şi $E = \{e\}$. Atunci E este subgrup al lui G, numit *subgrupul unitate*. În adevăr, dacă $x, y \in E$, atunci $x = y = e$, deci

$$x * y = e * e = e \in E,$$

$$x' = e' = e \in E.$$

Dacă G este dat în notaţie aditivă, atunci $0 = \{0\}$ este subgrup al lui G, numit *subgrupul zero*.

2. Fie $\mathfrak{S}_3$ grupul permutărilor de trei obiecte, $\mathfrak{S}_3 = \{e, \sigma, \pi, \alpha, \beta, \gamma\}$. Următoarele submulţimi ale lui $\mathfrak{S}_3$:

$$E = \{e\}, \ H_1 = \{e, \sigma, \pi\}, \ H_2 = \{e, \alpha\}, \ H_3 = \{e, \beta\}, \ H_4 = \{e, \gamma\}$$

sînt subgrupuri ale lui $\mathfrak{S}_3$. Să facem verificare pentru H_1. Din tabla operaţiei grupului $\mathfrak{S}_3$ se deduce că elementele lui H_1 se compun conform tablei următoare

$\circ$	e	σ	π
e	e	σ	π
σ	σ	π	e
π	π	e	σ

Se observă pe această tablă că H_1 este o parte stabilă a lui $\mathfrak{S}_3$ în raport cu compunerea precum şi cu operaţia de trecere la invers, deci H_1 este subgrup al lui $\mathfrak{S}_3$.

3. Fie $n \geqslant 0$ un număr întreg și $n\mathbf{Z}$ mulțimea tuturor multiplilor lui n,

$$n\mathbf{Z} \overset{\text{def}}{=} \{nh \mid h \in \mathbf{Z}\}.$$

Atunci $n\mathbf{Z}$ este subgrup al grupului $(\mathbf{Z}, +)$. În adevăr, dacă $x, y \in n\mathbf{Z}$, există $h, k \in \mathbf{Z}$ astfel încît $x = nh$, $y = nk$. Rezultă că

$$x + y = nh + nk = n(h + k) \in n\mathbf{Z},$$
$$-x = -(nh) = n(-h) \in n\mathbf{Z},$$

deci $n\mathbf{Z}$ este subgrup al lui $(\mathbf{Z}, +)$.

Fie $(G, \cdot)$ un grup, $a \in G$ și $n > 0$. Spunem că a este *element de ordin n* al grupului G dacă $a^n = e$ și $a^h \neq e$, $h = 1, 2, \ldots, n-1$.

Exerciții rezolvate

R – 1 Să se determine ordinul pentru fiecare element al grupului $\mathfrak{S}_3$.

Soluție. Pentru elementele lui $\mathfrak{S}_3$ păstrăm notațiile de la § 3. Folosind tabla operației grupului $\mathfrak{S}_3$ avem:

$$\sigma^1 = \sigma \neq e,\ \sigma^2 = \sigma \circ \sigma = \pi \neq e,\ \sigma^3 = \sigma^2 \circ \sigma = \pi \circ \sigma = e$$

deci σ este element de ordin 3. Analog se arată că π este element de ordin 3. Cum $\alpha^1 = \alpha$, $\alpha^2 = \alpha \circ \alpha = e$, rezultă că α este element de ordin 2. Analog se arată că β și γ sînt elemente de ordin 2. În fine, să observăm că într-un grup G elementul neutru este singurul element de ordin 1.

R – 2 Fie a un element de ordin n al unui grup $(G, \cdot)$.

1) Arătați că $H_a \overset{\text{def}}{=} \{e, a, a^2, \ldots, a^{n-1}\}$ este subgrup cu n elemente al lui G;

2) Dacă $\zeta = \cos\frac{2\pi}{n} + i \sin\frac{2\pi}{n}$, atunci ζ este element de ordin n al grupului $(\mathbf{C}^*, \cdot)$

3) Dacă $U_n = \{z \in \mathbf{C} \mid z^n = 1\}$, atunci U_n este subgrup cu n elemente al lui $(\mathbf{C}^*, \cdot)$, numit *grupul rădăcinilor de ordin n ale unității*;

4) Reprezentați geometric elementele grupului U_3 (resp. U_4, U_5).

Soluție. 1) Fie $x, y \in H$, $x = a^i$, $y = a^j$, unde $0 \leqslant i, j < n$. Fie $q, r \in \mathbf{Z}$ astfel încît $i + j = nq + r$, $0 \leqslant r < n$. Avem: $xy = a^i a^j = a^{i+j} = a^{nq+r} = (a^n)^q a^r = e^q a^r = a^r \in H_a$. Să mai observăm că inversele elementelor $e, a, a^2, \ldots, a^{n-1}$ sînt respectiv $e, a^{n-1}, a^{n-2}, \ldots, a \in H$, deci H este subgrup al lui G.

Dacă $a^i = a^j$, unde $0 \leqslant i, j < n$, atunci $i = j$. În adevăr, dacă $i < j$, atunci $0 < j - i < n$ și $a^{j-i} = a^j(a^i)^{-1} = a^j(a^j)^{-1} = e$, ceea ce nu este posibil căci ordinul lui a este n. Analog se arată că nu putem avea $i > j$. Deducem că elementele lui H_a sînt distincte.

2) Fie $h \in \mathbb{N}$, $0 \leqslant h < n$. Folosind formula lui Moivre, avem:

$$\zeta^h = \left(\cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n}\right)^h = \cos\frac{2h\pi}{n} + i\sin\frac{2h\pi}{n}.$$

Deducem că $\zeta^k \neq 1$ pentru $h = 1, 2, \ldots, n-1$ și $\zeta^n = 1$, deci ζ este element de ordin n al grupului $(\mathbb{C}^*, \cdot)$.

3) Este suficient să arătăm că $U_n = H_\zeta = \{1, \zeta, \zeta^2, \ldots, \zeta^{n-1}\}$, unde $\zeta = \cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n}$. Dacă $z \in H_\zeta$, atunci $z = \zeta^r$, $0 \leqslant r < n$, de unde $z^n = (\zeta^n)^r = 1^r = 1$, deci: $z \in U_n$. Așadar $H_\zeta \subseteq U_n$. Fie acum $z = \cos\varphi + i\sin\varphi \in U_n$. Cum $z^n = 1$, rezultă că $\cos n\varphi + i\sin n\varphi = 1$, deci $n\varphi = 2h\pi$, cu $h \in \mathbb{Z}$. Fie $q, r \in \mathbb{Z}$, astfel încît $h = nq + r$, $0 \leqslant r < n$.

Avem:

$$z = \cos\frac{2h\pi}{n} + i\sin\frac{2h\pi}{n} = \zeta^h = \zeta^{nq+r} = (\zeta^n)^q\zeta^r = \zeta^r \in H_\zeta,$$

de unde $U_n \subseteq H_\zeta$.

4) Se observă că reprezentînd numerele complexe din U_n punctele obținute sînt vîrfurile unui poligon regulat cu n laturi, cu centrul în origine și cu un vîrf în punctul de coordonate (1, 0) (v. fig. III.2).

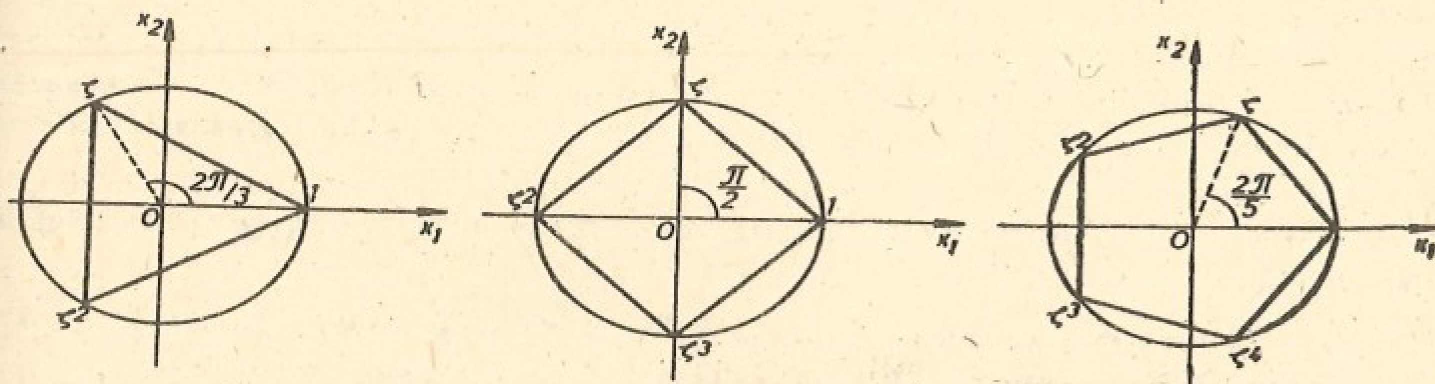


Fig. III.2.

§ 5. MORFISME DE GRUPURI

Numărul exemplelor de grupuri este considerabil și din acest motiv se impune o clasificare a acestora. Două grupuri G și Γ vor fi declarate ca fiind de același tip (*izotipice*) dacă sînt la fel de bogate în elemente și, mai puțin o bijecție $f: G \to \Gamma$, operațiile celor două grupuri acționează la fel asupra elementelor lui G, respectiv Γ. Mai precis:

5.1. *Definiție.* **Fie $(G, *)$ și $(\Gamma, \circ)$ două grupuri. O aplicație bijectivă $f: G \to \Gamma$ se numește *izomorfism* de grupuri dacă este și un morfism de grupuri, adică:**

$$f(x*y) = f(x)\circ f(y), \ \forall\ x, y \in G.$$

Spunem că un grup G este izomorf cu un grup Γ, și scriem $G \simeq \Gamma$, dacă există cel puțin un izomorfism $f: G \to \Gamma$. În caz contrar spunem că grupul G nu este izomorf cu grupul Γ și scriem $G \not\simeq \Gamma$.

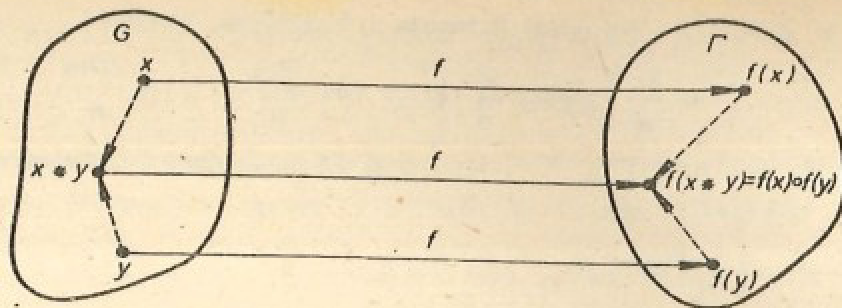


Fig. III.3.

Cu alți termeni, grupul $(G, *)$ este izomorf cu grupul $(\Gamma, \circ)$ dacă există o aplicație bijectivă $f \cdot G \to \Gamma$ astfel încît oricare ar fi $x, y \in G$ imaginea $f(x*y)$ a compusului $x*y$ prin f este egală cu compusul $f(x) \circ f(y)$ al imaginilor prin f ale lui x și y (v. fig. III.3) ; pe scurt : *imaginea compusului este egală cu compusul imaginilor*.

Dacă G și Γ sînt grupuri finite cu cîte n elemente, $G = \{a_1, a_2, \ldots, a_n\}$, $\Gamma = \{b_1, b_2, \ldots, b_n\}$, iar $f : G \to \Gamma$ este aplicația bijectivă definită prin

$$f(a_i) = b_i, \quad 1 \leqslant i \leqslant n$$

atunci f este izomorfism dacă și numai dacă pentru orice i și j, $1 \leqslant i, j \leqslant n$, imaginea prin f a elementului $a_i * a_j$ de la intersecția liniei lui a_i cu coloana lui a_j din tabla operației lui G coincide cu elementul $b_i \circ b_j$ de la intersecția liniei lui $b_i = f(a_i)$ cu coloana lui $b_j = f(a_j)$ din tabla operației lui Γ (v. fig. III.4).

Spunem în acest caz că tablele operațiilor celor două grupuri sînt *la fel structurate* (relativ la f).

5.2. Teoremă. Fie $(G, *)$ și $(\Gamma, \circ)$ două grupuri. Dacă $f : G \to \Gamma$ este izomorfism, atunci și $f^{-1} : \Gamma \to G$ este izomorfism.

Demonstrație. Fie $u, v \in \Gamma$. Cum f este aplicație bijectivă există $x, y \in G$ unic determinați astfel încît $f(x) = u$ si $f(y) = v$. Conform definiției aplicației f^{-1} avem $f^{-1}(u) = x$ și $f^{-1}(v) = y$.

Dar

$$u \circ v = f(x) \circ f(y) = f(x*y),$$

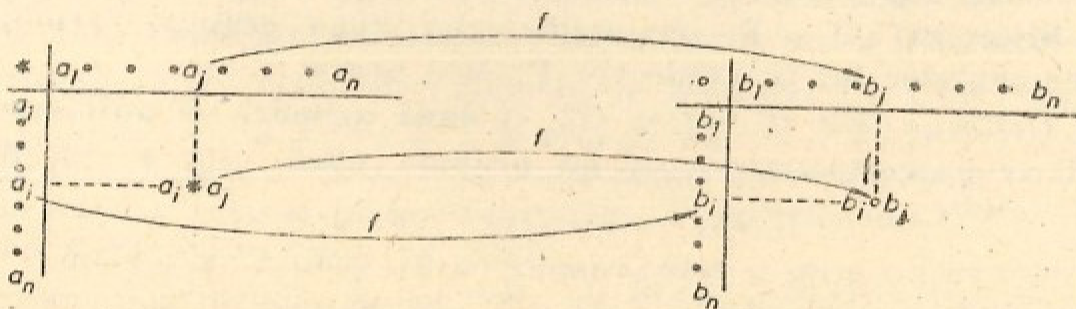


Fig. III.4.

de unde

$$f^{-1}(u \circ v) = x * y = f^{-1}(u) * f^{-1}(v)$$

și cum f^{-1} este aplicație bijectivă, rezultă că f^{-1} este izomorfism.

Exemple

1. $(\mathbf{R}, +) \simeq (\mathbf{R}_+^*, \cdot)$. *Grupul aditiv* $(\mathbf{R}, +)$ *al numerelor reale este* **izomorf** *cu grupul multiplicativ* $(\mathbf{R}_+^*, \cdot)$ *al numerelor reale strict pozitive.*

   În adevăr, fie $a \in \mathbf{R}$, $a > 0$, $a \neq 1$ și $f : \mathbf{R} \to \mathbf{R}_+^*$,

$$f(x) = a^x, \quad \forall\, x \in \mathbf{R}.$$

   Cum f este aplicație bijectivă și

$$f(x + y) = a^{x+y} = a^x a^y = f(x)\, f(y), \ \forall\, x, y \in \mathbf{R},$$

   rezultă că f este izomorfism.

   Să observăm în acest caz că inversul izomorfismului f este aplicația $f^{-1} : \mathbf{R}^*_+ \to \mathbf{R}$,

$$f^{-1}(x) = \log_a x, \ \forall\, x \in \mathbf{R}_+^*$$

și avem :

$$f^{-1}(xy) = \log_a(xy) = \log_a x + \log_a y = f^{-1}(x) + f^{-1}(y), \ \forall\, x, y \in \mathbf{R}_+^*.$$

   Între două grupuri pot exista mai multe izomorfisme, în cazul de față chiar o infinitate (la orice $a > 0$, $a \neq 1$, corespunde un izomorfism).

2. $(\mathbf{Q}, +) \not\simeq (\mathbf{Q}_+^*, \cdot)$. *Grupul aditiv* $(\mathbf{Q}, +)$ *al numerelor raționale nu este izomorf* cu grupul multiplicativ $(\mathbf{Q}_+^*, \cdot)$ *al numerelor raționale strict pozitive*.

   În adevăr, dacă $f : \mathbf{Q} \to \mathbf{Q}_+^*$, este un izomorfism între aceste două grupuri, există $r \in \mathbf{Q}$ astfel încît $f(r) = 2$. Cum $f(r/2) \in \mathbf{Q}$ și

$$2 = f(r) = f\left(\frac{r}{2} + \frac{r}{2}\right) = f\left(\frac{r}{2}\right) f\left(\frac{r}{2}\right) = \left(f\left(\frac{r}{2}\right)\right)^2$$

   rezultă că $\sqrt{2} \in \mathbf{Q}$. Contradicție.

3. *Dacă* $(G, *)$ și $(\Gamma, \circ)$ *sînt două grupuri cu cîte trei elemente, atunci* $G \simeq \Gamma$. Cu alte cuvinte, există un singur tip de grup cu trei elemente.

   În adevăr, fie $G = \{e, a, b\}$, $\Gamma = \{\theta, u, v\}$ unde e și θ sînt elementele neutre ale lui G și Γ respectiv. Pentru că e și θ sînt elemente neutre, în tablele operațiilor celor două grupuri putem completa următoarele poziții :

$*$	e	a	b
e	e	a	b
a	a	?	?
b	b	?	?

$\circ$	θ	u	v
θ	θ	u	v
u	u	?	?
v	v	?	?

Avem $a*a = b$. În adevăr, nu putem avea $a*a = a$ căci a s-ar repeta în linia sa. De asemenea, nu putem avea $a*a = e$ căci atunci, ca să evităm repetarea lui a și e în linia lui a, am fi obligați să punem $a*b = b$, ceea ce produce o repetare a lui b în coloana acestuia.

Cum $a*a = b$, pentru a evita repetarea elementelor lui G, în liniile și coloanele tablei operației acestuia, trebuie să avem $a*b = e$, $b*a = e$, $b*b = a$. Analog, se completează tabla operației lui Γ.

$*$	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

$\circ$	θ	u	v
θ	θ	u	v
u	u	v	θ
v	v	θ	u

Definind $f : G \to \Gamma$ prin $f(e) = \theta$, $f(a) = u$ și $f(b) = v$, rezultă că f este izomorfism de grupuri căci f este aplicație bijectivă și tablele operațiilor celor două grupuri sînt la fel structurate (relativ la f).

Renunțînd la condiția de bijectivitate din definiția izomorfismului se obține noțiunea mai generală de *morfism* (*omomorfism*) de grupuri, anume:

5.3. *Definiție*. **Fie $(G, *)$ și $(\Gamma, \circ)$ două grupuri. O aplicație $f : G \to \Gamma$ se numește morfism de grupuri dacă**

$$f(x*y) = f(x)\circ f(y), \quad \forall\ x, y \in G.$$

Evident, orice izomorfism de grupuri este morfism de grupuri.

Aplicația $f : \mathbf{Z} \to \mathcal{R}_4$ de la grupul $(\mathbf{Z}, +)$ la grupul $(\mathcal{R}_4, \oplus)$,

$$f(a) = a \text{ mod } 4, \quad \forall\ a \in \mathbf{Z}$$

este un morfism de grupuri. În adevăr, dacă $a, b \in \mathbf{Z}$, fie $a_1 = a$ mod 4, $b_1 = b$ mod 4. Există $h, k \in \mathbf{Z}$ astfel încît:

$$a = 4h + a_1, \quad b = 4k + b_1$$

și conform Lemei 8.1 Cap. II avem:

$$a \oplus b = a_1 \oplus b_1.$$

Rezultă că:

$$f(a + b) = (a + b) \text{ mod } 4 = a \oplus b = a_1 \oplus b_1 = f(a) \oplus f(b), \quad \forall\ a, b \in \mathbf{Z},$$

deci f este morfism de grupuri. Se observă că f este morfism surjectiv dar nu este injectiv.

Astfel:

$$f(7) = 7 \text{ mod } 4 = 3 = 19 \text{ mod } 4 = f(19).$$

5.4. **Teoremă. Fie $(G, *)$ și $(\Gamma, \circ)$ două grupuri, e și θ elementele neutre ale lui G și Γ respectiv. Dacă $f : G \to \Gamma$ este un morfism de grupuri, atunci:**

1) $f(e) = \theta$;

2) $f(x') = (f(x))' \quad \forall\ x \in G$,

unde x' este simetricul lui x iar $(f(x))'$ este simetricul lui $f(x)$.

Demonstrație. 1) Avem :

$$\theta \circ f(e) = f(e) = f(e * e) = f(e) \circ f(e)$$

și prin simplificare cu $f(e)$ se obține $\theta = f(e)$.

2) Pentru orice $x \in G$ avem :

$$\theta = f(e) = f(x * x') = f(x) \circ f(x')$$

deci $\theta = f(x) \circ f(x')$ și analog $f(x') \circ f(x) = \theta$, de unde $(f(x))' = f(x')$.

Fie G un grup. Un izomorfism (morfism) $f : G \to G$ se numește *automorfism* (resp. *endomorfism*) al grupului G.

Exerciții rezolvate

R — 1 Fie $(G, *)$ un grup cu patru elemente astfel încît $x^2 = e$, $\forall x \in G$, unde e este elementul neutru.

1) Arătați că $G \simeq \mathcal{K}$, unde $\mathcal{K}$ este grupul lui Klein (v. § 3).

2) Arătați că grupul $(G, *)$ nu este izomorf cu grupul $(\mathcal{R}_4, \oplus)$.

Soluție. 1) Fie $G = \{e, a, b, c\}$. Tablele operațiilor grupurilor G și $\mathcal{K}$ sînt (v. § 3 și Ex. **R – 3**, § 4) :

$*$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

$\circ$	1_E	u	v	w
1_E	1_E	u	v	w
u	u	1_E	w	v
v	v	w	1_E	u
w	w	v	u	1_E

Aplicația $f : G \to \mathcal{K}$ definită prin $f(e) = 1_E$, $f(a) = n$, $f(b) = v$, $f(c) = w$ este izomorfism căci tablele operațiilor celor două grupuri sînt la fel de structurate (relativ la f).

2) În adevăr, să presupunem că există un izomorfism $f : G \to \mathcal{R}_4$ și fie $x \in G$ astfel încît $f(x) = 3$. Atunci :

$$0 = f(e) = f(x * x) = f(x) \oplus f(x) = 3 \oplus 3 = 2.$$

Contradicție.

R — 2 Arătați că aplicația $f : \mathbf{Z} \to \mathbf{C}^*$,

$$f(h) = \cos\frac{2h\pi}{n} + i\sin\frac{2h\pi}{n}, \quad \forall h \in \mathbf{Z}$$

este un morfism de la grupul $(\mathbf{Z}, +)$ la grupul $(\mathbf{C}^*, \cdot)$.

Determinați numerele $x \in \mathbf{Z}$ astfel încît $f(x) = 1$.

Soluție. Pentru orice $h, k \in \mathbf{Z}$ avem :

$$f(h + k) = \cos\frac{2(h + k)\pi}{n} + i\sin\frac{2(h + k)\pi}{n} = \left(\cos\frac{2h\pi}{n} + i\sin\frac{2h\pi}{n}\right) \cdot$$

$$\cdot \left(\cos\frac{2k\pi}{n} + i\sin\frac{2k\pi}{n}\right) = f(h)f(k)$$

și deci f este morfism de la grupul $(\mathbf{Z}, +)$ la grupul $(\mathbf{C}^*, \cdot)$.

Se observă că pentru $x \in \mathbf{Z}$ avem $f(x) = 1$ dacă și numai dacă

$$\cos\frac{2x\pi}{n} + i\sin\frac{2x\pi}{n} = 1$$

ceea ce este posibil dacă și numai dacă

$$\frac{2x\pi}{n} = 2\pi k, \quad k \in \mathbf{Z}.$$

Rezultă că $f(x) = 1$ dacă și numai dacă $x = nk$, $k \in \mathbf{Z}$, deci $f(x) = 1$ dacă și numai dacă $n \mid x$.

R — 3 Pentru orice $a \in \mathbf{R}$, definim $t_a : \mathbf{R} \to \mathbf{R}$, $t_a(x) = x + a$, $\forall\, x \in \mathbf{R}$. Arătați că :

1) Mulțimea $\mathcal{F}(R) = \{t_a \mid a \in \mathbf{R}\}$ este grup în raport cu compunerea funcțiilor.

2) Grupul $(\mathbf{R}, +)$ este izomorf cu grupul $(\mathcal{F}(\mathbf{R}), \circ)$.

Soluție. 1) Pentru $a, b \in \mathbf{R}$, avem $t_a \circ t_b = t_{a+b}$. În adevăr, oricare ar fi $x \in \mathbf{R}$ avem:

$$(t_a \circ t_b)(x) = t_a(t_b(x)) = t_a(x + b) = x + b + a = t_{a+b}(x),$$

de unde $t_a \circ t_b = t_{a+b}$, deci compunerea funcțiilor induce o lege de compoziție pe $\mathcal{F}(\mathbf{R})$ evident asociativă și cu element neutru, egal cu $1_{\mathbf{R}} = t_0 \in \mathcal{F}(\mathbf{R})$.

Cum

$$t_a \circ t_{-a} = t_{a+(-a)} = t_0 = t_{(-a)+a} = t_{-a} \circ t_a, \ \forall\, a \in \mathbf{R},$$

rezultă că $t_a^{-1} = t_{-a}$, $\forall\, a \in \mathbf{R}$, deci $(\mathcal{F}(\mathbf{R}), \circ)$ este grup.

2) Funcția $f : \mathbf{R} \to \mathcal{F}(\mathbf{R})$, $f(a) = t_a$, este bijectivă și

$$f(a + b) = t_{a+b} = t_a \circ t_b = f(a) \circ f(b), \ \forall\, a, b \in \mathbf{R}.$$

Exerciții

1. Fie $M = \mathbf{Z}[i] = \{a + bi \mid a, b \in \mathbf{Z}\}$.

1) Arătați că M este o parte stabilă a lui $\mathbf{C}$ în raport cu înmulțirea și că formează monoid comutativ în raport cu operația indusă.

2) Determinați elementele simetrizabile ale monoidului $(M, \cdot)$.

2. Arătați că corespondența $(x, y) \to x * y \overset{\text{def}}{=} (x + y) / (1 + xy)$ este o lege de compoziție pe intervalul $G = (-1, 1)$ și că $(G, *)$ este grup abelian.

3. Fie $\varepsilon = -1/2 + i\sqrt{3/2}$ și $G = \{1, \varepsilon, \varepsilon^2\} \subset \mathbf{C}$.

1) Arătați că G este o parte stabilă a lui $\mathbf{C}$ în raport cu înmulțirea și alcătuiți tabla operației induse.

2) Deduceți că $(G, \cdot)$ este grup abelian.

4. Fie $E = \mathbf{R} \setminus \{0\}$ și $f_i : E \to E$, $1 \leqslant i \leqslant 4$,

$$f_1(x) = x, \quad f_2(x) = \frac{1}{x}, \quad f_3(x) = -x, \quad f_4(x) = -\frac{1}{x}, \ \forall\, x \in E.$$

1) Arătați că mulțimea $G = \{f_1, f_2, f_3, f_4\}$ este stabilă în raport cu compunerea funcțiilor și alcătuiți tabla operației induse.

2) Deduceți că $(G, \circ)$ este grup abelian.

5. Fie $E = \mathbf{R} \setminus \{0, 1\}$ și $f_i : E \to E$ $1 \leqslant i \leqslant 6$,

$$f_1(x) = x,\ f_2(x) = \frac{1}{1-x},\ f_3(x) = \frac{x-1}{x},\ f_4(x) = \frac{1}{x},\ f_5(x) = 1 - x,$$

$$f_6(x) = \frac{x}{x-1}, \quad \forall\, x \in E.$$

1) Arătați că mulțimea $G = \{f_1, f_2, f_3, f_4, f_5, f_6\}$ este stabilă în raport cu compunerea funcțiilor și alcătuiți tabla operației induse.

2) Deduceți că $(G, \circ)$ este grup necomutativ.

6. Fie $G = (0, \infty) \setminus \{1\}$. Arătați că corespondența

$$(x, y) \to x * y \overset{\text{def}}{=\!=} x^{\ln y}$$

este o lege de compoziție pe G și că $(G, *)$ este grup comutativ.

7. Fie $G = [-1, \infty)$, $\Gamma = (-1, \infty)$ și următoarea lege de compoziție pe $\mathbf{R}$,

$$(x, y) \to x * y \overset{\text{def}}{=\!=} x + y + xy.$$

1) Arătați că G și Γ sînt părți stabile ale lui $\mathbf{R}$ în raport cu legea de compoziție „$*$".

2) Dacă „$\top$", și „$\perp$" sînt legile de compoziție induse pe G respectiv Γ, de „$*$" atunci $(G, \top)$ și $(\Gamma, \perp)$ sînt monoizi comutativi.

3) Care dintre monoizii $(G, \top)$ și $(\Gamma, \perp)$ este grup?

8. Pe $\mathbf{Z}$ se definește legea de compoziție

$$\mathbf{Z} \times \mathbf{Z} \to \mathbf{Z},\ (x, y) \to x \perp y \overset{\text{def}}{=\!=} x + y - 1.$$

Arătați că $(\mathbf{Z}, \perp)$ este grup abelian.

9. Fie $(G, *)$ un grup comutativ și $a \in G$. Pe G se definește legea de compoziție

$$G \times G \to G,\ (x, y) \to x \perp y \overset{\text{def}}{=\!=} x * y * a.$$

Arătați că $(G, \perp)$ este grup.

10. Fie $(G, \cdot)$ un grup cu proprietatea:

$$(xy)^2 = x^2y^2, \quad \forall\, x, y \in G.$$

Arătați că G este grup abelian.

11. Fie $(G, \cdot)$ un grup cu proprietatea:

$$x^2 = e, \quad \forall\, x \in G.$$

Arătați că G este grup abelian.

12. Fie $(G, \perp)$ și $(G, \top)$ două structuri de grup definite pe aceeași mulțime. Dacă legile de compoziție „$\perp$" și „$\top$" au același element neutru și

$$x \perp y = (x \top x) \top (x \top y), \quad \forall, x, y \in G$$

atunci:

1) $x \perp y = x \top y$, $\quad \forall\, x, y \in G$

2) $x \perp y = y \perp x$, $\quad \forall\, x, y \in G$,

13. Fie $\sigma, \gamma \in \mathfrak{S}_3$, $\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ $\gamma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$

Să se găsească $\xi \in \mathfrak{S}_3$ astfel încît $\sigma \circ \xi = \gamma$.

14. Fie $\sigma, \pi \in \mathfrak{S}_4$, $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$, $\pi = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{pmatrix}$.

1) Arătați că $\sigma^4 = e$ și $\pi^3 = e$, unde e este permutarea identică.

2) Rezolvați în $\mathfrak{S}_4$ ecuațiile: $\sigma^{129} \circ x = \pi^{101}$ și $y \circ \sigma^{207} = \pi^{63}$.

15. Fie $(G, \cdot)$ un grup și $a, b \in G$ astfel încît $ab = ba$. Să se arate că:

$$a^h b^k = b^k a^h, \quad \forall\ h, k \in \mathbf{Z}.$$

16. Fie $(G, \cdot)$ un grup și e elementul său neutru. Dacă elementele $a, b \in G$ satisfac condițiile

$$b^6 = e, \quad ab = b^4 a$$

atunci $b^3 = e$ și $ab = ba$.

17. Fie $(G, *)$ un grup și $a \in G$. Arătați că funcțiile:

$$f : G \to G, \quad f(x) = a * x, \quad \forall\ x \in G$$

$$g : G \to G, \quad g(x) = x * a, \quad \forall\ x \in G$$

sînt bijective.

18. Fie $$H_1 = \left\{ A \in M_2(\mathbf{Z}) \,\middle|\, A = \begin{pmatrix} 0 & a \\ 0 & b \end{pmatrix} \right\} \text{ și}$$

$$H_2 = \left\{ A \in M_2(\mathbf{Z}) \,\middle|\, A = \begin{pmatrix} 2a & 3b \\ 4c & 5d \end{pmatrix},\ a, b, c, d \in \mathbf{Z} \right\}.$$

1) Arătați că $M_2(\mathbf{Z})$ este grup în raport cu adunarea matricelor.
2) H_1 și H_2 sînt subgrupuri ale grupului $(M_2(\mathbf{Z}), +)$.

19. 1) Dacă H_1 și H_2 sînt subgrupuri ale unui grup G, atunci $H_1 \cap H_2$ este subgrup al lui G.
2) Arătați că pentru subgrupurile $3\mathbf{Z}$ și $4\mathbf{Z}$ ale grupului $(\mathbf{Z}, +)$ avem:

$$3\mathbf{Z} \cap 4\mathbf{Z} = 12\mathbf{Z}.$$

20. Fie $f : \mathbf{R} \to \mathbf{R}$ o funcție reală cu proprietatea că există cel puțin un număr $T \in \mathbf{R}^*$ astfel încît

$$(*) \qquad f(x + T) = f(x), \quad \forall\ x \in \mathbf{R}.$$

1) Arătați că mulțimea H a numerelor reale T cu proprietatea $(*)$ este subgrup al grupului $(\mathbf{R}, +)$.

2) Determinați acest subgrup cînd

a) $f(x) = \sin 2\pi x, \quad \forall\ x \in \mathbf{R}$;

b) $f(x) = \begin{cases} 1, & x \in \mathbf{Q} \\ 0, & x \in \mathbf{R} \setminus \mathbf{Q}. \end{cases}$

21. Arătați că grupul $(G, \cdot)$ de la Ex. 3 este izomorf cu grupul $(\mathcal{R}_3, \oplus)$.

22. Arătați că grupul lui Klein este izomorf cu grupul $(G, \circ)$ de la Ex. 4.

23. Arătați că grupul $(\mathfrak{S}_3, \circ)$ este izomorf cu grupul $(G, \circ)$ de la Ex. 5.

24. Arătați că funcția $f : (0, \infty) \to (-1, 1)$,

$$f(x) = \frac{x - 1}{x + 1}, \quad \forall\ x \in (0, \infty)$$

este un izomorfism de la grupul $(\mathbf{R}_+^*, \cdot)$ la grupul $(G, *)$ de la Ex. 2.

25. Fie $G = \left(-\frac{\pi}{2}, \frac{\pi}{2}\right)$ şi pentru orice $x, y \in G$ fie

$f(x) = tg\, x$ (pt. b)

$$x * y \stackrel{\text{def}}{=} \operatorname{arctg}(\operatorname{tg} x + \operatorname{tg} y).$$

Arătaţi că $(G, *)$ este grup şi că $(G, *) \simeq (\mathbf{R}, +)$. (b)

26. Fie $R_\theta = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$, $\theta \in \mathbf{R}$ (v. Ex. 6, Cap. I)

şi $G = \{E, A, B, C\}$, unde $E = R_0$, $A = R_{\pi/2}$, $B = R_\pi$ şi $C = R_{3\pi/2}$.

1) Arătaţi că G este o parte stabilă a lui $M_2(\mathbf{R})$ în raport cu înmulţirea şi alcătuiţi tabla operaţiei induse.

2) Deduceţi că $(G, \cdot)$ este grup şi arătaţi că $(G, \cdot) \simeq (\mathcal{R}_4, \overset{\prime}{\oplus})$.

27. Arătaţi că funcţia $f : \mathbf{Z} \to \mathbf{Q}$,

$f(k) = (-1)^k$, $\forall k \in \mathbf{Z}$, este morfism de la grupul $(\mathbf{Z}, +)$ la grupul $(\mathbf{Q}^*, \cdot)$.

28. Fie E o mulţime cu două elemente, $E = \{a, b\}$. Pe mulţimea $\mathfrak{P}(E)$ definim legea de compoziţie „Δ", numită *diferenţa simetrică a două mulţimi*.

$$X \,\Delta\, Y = (X \setminus Y) \cup (Y \setminus X), \ \forall\ X, Y \in \mathfrak{P}(E).$$

1) Alcătuiţi tabla legii de compoziţie „Δ";
2) Comparaţi tabla operaţiei „Δ" cu tabla grupului $\mathcal{K}$ al lui Klein (v. § 3) şi indicaţi o funcţie bijectivă $f : \mathcal{K} \to \mathfrak{P}(E)$ astfel încît:

$$f(x \circ y) = f(x) \Delta f(y), \ \forall\ x, y \in \mathcal{K};$$

3) Deduceţi că $(\mathfrak{P}(E), \Delta)$ este grup.

29. Fie $E = \mathbf{R} \times \mathbf{R}$. Pentru orice $t \in \mathbf{R}$ fie funcţia

$$f_t : E \to E,$$

$$f_t(x, y) = \left(x + ty + \frac{t^2}{2}, y + t\right), \ \forall\ (x, y) \in E.$$

Arătaţi că:

1) $f_t \circ f_{t'} = f_{t+t'}$, $f_0 = 1_E$, $f_t^{-1} = f_{-t}$.
2) Mulţimea $G = \{f_t : |\ t \in \mathbf{R}\}$ este grup în raport cu operaţia de compunere a funcţiilor.
3) $(G, \circ) \simeq (\mathbf{R}, +)$.

* * *

30*. Fie $R_\theta = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$, $S_\theta = \begin{pmatrix} \cos\theta & \sin\theta \\ \sin\theta & -\cos\theta \end{pmatrix}$,

$\theta \in \mathbf{R}$ (v. Ex. 6, Cap. I) şi $G = \{E, A, B, U, V, W\}$ unde

$E = R_0$, $A = R_{2\pi/3}$, $B = R_{4\pi/3}$; $U = S_0$, $V = S_{4\pi/3}$, $W = S_{2\pi/3}$.

1) Arătaţi că G este parte stabilă a lui $M_2(\mathbf{R})$ în raport cu înmulţirea şi alcătuiţi tabla operaţiei induse.

2) Deduceţi că G este grup şi că $(G, \cdot) \simeq (\mathfrak{S}_3, \circ)$.

31*. Fie $(G, \cdot)$ un grup şi H o submulţime finită a lui G. Următoarele afirmaţii sînt echivalente:

1) $\forall\ x, y \in H \Rightarrow xy \in H$;

2) H este subgrup al lui G.

32*. Fie G o mulţime şi $G \times G \to G$, $(x, y) \to xy$ o lege de compoziţie asociativă. Următoarele afirmaţii sînt echivalente:

1) $(G, \cdot)$ este grup;

2) $\forall\ a, b \in G$ există $x, y \in G$ astfel încît $ax = b$ şi $ya = b$.

33*. Fie H o submulţime nevidă a lui $\mathbb{Z}$. Următoarele afirmaţii sînt echivalente:

1) H este subgrup al lui $\mathbb{Z}$;

2) $\exists\ n \geqslant 0$ astfel încît $H = n\mathbb{Z}$.

34*. Fie $z \in \mathbb{C}$. Arătaţi că există $n > 0$ astfel încît $z^n = 1$ dacă şi numai dacă $z = \cos 2r\pi + i \sin 2r\pi$, cu $r \in \mathbb{Q}$.

35*. Fie H un subgrup cu n elemente al grupului $(\mathbb{C}^*, \cdot)$. Arătaţi că $H = U_n$, unde U_n este grupul rădăcinilor de ordin n ale unităţii.

36*. Determinaţi automorfismele grupului $(\mathbb{Z}, +)$.

§ 1. DEFINIŢIA INELULUI. EXEMPLE

Vom studia în continuare o nouă structură algebrică — structura de *inel*. Noţiunea de inel s-a degajat iniţial în cadrul teoriei numerelor, unde a apărut sub numele de *inel de numere*, prototipul fiind $\mathbf{Z}$ luat împreună cu operaţiile de adunare şi înmulţire a numerelor întregi,

$$\mathbf{Z} \times \mathbf{Z} \to \mathbf{Z},\ (x, y) \to x + y,$$

respectiv

$$\mathbf{Z} \times \mathbf{Z} \to \mathbf{Z},\ (x, y) \to xy.$$

Ulterior, noţiunea de inel a avut numeroase aplicaţii în diferite domenii ale Algebrei (inele de polinoame, inele de matrice) în Analiză (inele de funcţii) în Logică (inele booleene) etc.

1.1. *Definiţie.* **O mulţime nevidă A, luată împreună cu două legi de compoziţie** *(adunarea şi înmulţirea)*

$$A \times A \to A,\ (x, y) \to x + y$$

şi

$$A \times A \to A,\ (x, y) \to xy,$$

se numeşte *inel* **dacă :**

G) **$(A, +)$ este grup abelian,**

M) **$(A, \cdot)$ este monoid,**

D) **înmulţirea este distributivă faţă de adunare, anume :**

$$x(y + z) = xy + xz,\ (y + z)x = yx + zx\ \forall x, y, z \in A,$$

Afirmaţia că $(A, +)$ este grup abelian revine la faptul că adunarea inelului satisface axiomele :

G_1) $(x + y) + z = x + (y + z)\ \forall x, y, z \in A,$

G_2) $\exists\ 0 \in A$ astfel încît $0 + x = x + 0 = x\ \forall\ x \in A,$

G_3) $\forall\ x \in A,\ \exists\ x' = A$ astfel încît $x' + x = x + x' = 0,$

G_4) $x + y = y + x\ \forall x, y \in A.$

Afirmaţia că $(A, \cdot)$ este monoid revine la faptul că înmulţirea inelului satisface axiomele :

M_1) $(xy)z = x(yz)\ \forall x, y, z \in A,$

M_2 $\exists\ 1 \in A$ astfel încît $1 \cdot x = x \cdot 1 = x\ \forall x \in A.$

Vom spune că $(A, +)$ este *grupul aditiv* al inelului A. Ansamblul de condiţii G_1—G_4, M_1, M_2 şi D poartă numele de *axiomele inelului*. Elemen-

tele 0 și 1 sînt unic determinate și se numesc *elementul zero*, respectiv *elementul unitate* al inelului A. Inelul A se numește *finit* dacă A are doar un număr finit de elemente. Elementele $x \in A$ simetrizabile în raport cu înmulțirea lui A se numesc *elemente inversabile* sau *unități* ale inelului A.

Dacă înmulțirea inelului satisface încă și axioma:

M_4) $xy = xy \ \forall x, y \in A$

spunem că A este *inel comutativ*.

Spunem că A este *inel fără divizori* ai lui zero dacă

$$x \neq 0 \text{ și } y \neq 0 \Rightarrow xy \neq 0.$$

Un inel comutativ cu cel puțin două elemente și fără divizori ai lui zero se numește *domeniu de integritate*.

Exemple

1. *Inelul* **Z** *al întregilor raționali*. Din proprietățile adunării și înmulțirii numerelor întregi, enumerate în Cap. I, § 1, rezultă că $(\mathbf{Z}, +, \cdot)$ este inel comutativ, numit *inelul întregilor raționali*.
2. *Inelul* **Z**[i] *al întregilor lui Gauss*. Fie **Z**[i] mulțimea tuturor numerelor complexe de forma $a + bi$, cu $a, b \in \mathbf{Z}$, numite *întregi ai lui Gauss*. Dacă $a + bi$ și $c + di$ sînt din **Z**[i], atunci

$$(a + bi) + (c + di) = (a + c) + (b + d)\mathrm{i} \in \mathbf{Z}[\mathrm{i}]$$

și

$$(a + bi)(c + di) = (ac - bd) + (ad + bc)\mathrm{i} \in \mathbf{Z}[\mathrm{i}].$$

Rezultă că **Z**[i] este o parte stabilă a lui **C** în raport cu adunarea și înmulțirea numerelor complexe. Evident, operațiile induse verifică axiomele G_1, G_4, M_1, M_3 și D.

Cum $0 = 0 + 0 \cdot \mathrm{i}$ și $1 = 1 + 0 \cdot \mathrm{i}$, rezultă că aceste operații verifică și axiomele G_2 și M_2. În fine, pentru orice $z \in \mathbf{Z}[\mathrm{i}]$, $z = a + \mathrm{i}b$, avem $-z = (-a) + (-b)\mathrm{i} \in \mathbf{Z}[\mathrm{i}]$, deci este verificată și axioma G_2. Așadar **Z**[i] este inel comutativ în raport cu operațiile induse pe **Z**[i] de adunarea și înmulțirea numerelor complexe, numit *inelul întregilor lui Gauss*.

3. *Inelul* $(\mathcal{R}_n, \oplus, \otimes)$ *al resturilor modulo* n. Fie n un număr întreg pozitiv și $\mathcal{R}_n = \{0, 1, 2, \ldots, n - 1\} \subset \mathbf{Z}$. Operațiile induse pe $\mathcal{R}_n$ de adunarea și înmulțirea modulo n satisfac axiomele inelului comutativ (v. § 8, Cap. II). Așadar, $\mathcal{R}_n$ este inel comutativ în raport cu adunarea și înmulțirea modulo n, numit *inelul resturilor modulo* n.

Un interes aparte, prin aplicațiile pe care le are în diferite domenii ale tehnicii (aritmetica calculatoarelor, teoria codurilor) îl prezintă inelul $(\mathcal{R}_2, \oplus, \otimes)$

$\oplus$	0	1
0	0	1
1	1	0

$\otimes$	0	1
0	0	0
1	0	1

Tablele operațiilor inelului $\mathcal{R}_2 = \{0, 1\}$.

În inelul $\mathscr{R}_6$ avem $2 \otimes 3 = 0$, $4 \otimes 3 = 0$, deci $(\mathscr{R}_6, \oplus, \otimes)$ este inel cu divizori ai lui zero.

4. $(\mathbf{Q}, +, \cdot)$, $(\mathbf{R}, +, \cdot)$ și $(\mathbf{C}, +, \cdot)$ sînt inele comutative (v. Cap. I, § 1). Să observăm că pentru orice $x \neq 0$ din $\mathbf{Q}$, $\mathbf{R}$ sau $\mathbf{C}$ există $y \neq 0$ din $\mathbf{Q}$, $\mathbf{R}$ respectiv $\mathbf{C}$, astfel încît $xy = 1$. Inelele cu această proprietate suplimentară vor fi studiate mai tîrziu.

5. *Inelul matricelor pătratice.* Fie A un inel. Inelul A poate fi oricare din inelele $\mathbf{Z}$, $\mathbf{Z}[i]$, $\mathscr{R}_n$, $\mathbf{Q}$ etc. Notăm cu $M_2(A)$ mulțimea tuturor matricelor U pătratice de ordin 2 cu coeficienți din A,

$$U = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}, \ a_{ij} \in A.$$

Dacă $U, V \in M_2(A)$,

$$U = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}, \ V = \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix}$$

definim matricele $U + V$ și UV prin

$$U + V \overset{\text{def}}{=} \begin{pmatrix} a_{11} + b_{11} & a_{12} + b_{12} \\ a_{21} + b_{21} & a_{22} + b_{22} \end{pmatrix} \in M_2(A)$$

și

$$UV \overset{\text{def}}{=} \begin{pmatrix} a_{11}b_{11} + a_{12}b_{21} & a_{11}b_{12} + a_{12}b_{22} \\ a_{21}b_{11} + a_{22}b_{21} & a_{21}b_{12} + a_{22}b_{22} \end{pmatrix} \in M_2(A).$$

Matricele 0, E și $-U$ din $M_2(A)$,

$$0 = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \ E = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \ -U = \begin{pmatrix} -a_{11} & -a_{12} \\ -a_{21} & -a_{22} \end{pmatrix}$$

se numesc respectiv *matricea zero, matricea unitate, opusa* matricei U.

Am amintit o serie de proprietăți ale adunării și înmulțirii matricelor din $M_2(\mathbf{R})$. Demonstrațiile multora dintre ele se fac invocînd proprietăți ale adunării și înmulțirii numerelor reale, care sînt de asemenea adevărate pentru adunarea și înmulțirea oricărui inel A. Din acest motiv, asemenea demonstrații pot fi reproduse și pentru matricele din $M_2(A)$. Pe această cale se poate demonstra :

G_1) $(U + V) + W = U + (V + W)$,

G_2) $0 + U = U + 0 = U$,

G_3) $U + (-U) = (-U) + U = 0$,

G_4) $U + V = V + U$,

M_1) $(UV)W = U(VW)$,

M_2) $EU = UE = U$,

D) $U(V + W) = UV + UW$; $(V + W)U = VU + WU$

oricare ar fi $U, V, W \in M_2(A)$.

Rezultă că adunarea şi înmulţirea matricelor conferă lui $M_2(A)$ o structură de inel.

La fel se organizează ca inel mulţimea $M_n(A)$ a matricelor pătratice de ordin n cu coeficienţi din A.

Cînd $n > 1$, inelul $M_n(A)$ nu este comutativ şi are divizori ai lui zero.

Astfel, dacă $U, V \in M_2(\mathcal{R}_6)$,

$$U = \begin{pmatrix} 1 & 3 \\ 3 & 3 \end{pmatrix}, V = \begin{pmatrix} 3 & 0 \\ 3 & 2 \end{pmatrix}$$

atunci

$$UV = \begin{pmatrix} 1 & 3 \\ 3 & 3 \end{pmatrix}\begin{pmatrix} 3 & 0 \\ 3 & 2 \end{pmatrix} = \begin{pmatrix} 1 \otimes 3 \oplus 3 \otimes 3 & 1 \otimes 0 \oplus 3 \otimes 2 \\ 3 \otimes 3 \oplus 3 \otimes 3 & 3 \otimes 0 \oplus 3 \otimes 2 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

deci inelul $M_2(\mathcal{R}_6)$ are divizori ai lui zero.

§ 2. REGULI DE CALCUL ÎNTR-UN INEL

Calculul algebric cu elementele unui inel beneficiază de toate regulile date pentru grupuri şi monoizi dacă sînt implicate separat adunarea, respectiv înmulţirea inelului. În afară de acestea, într-un inel avem o serie de reguli de calcul specifice, care se referă la ansamblul celor două operaţii ale inelului.

1. *Pentru orice $x \in A$ avem*: $x0 = 0x = 0$. În adevăr, fie $y = x0$. Cum $x0 = x(0+0) = x0 + x0$, avem $y = y + y$. Atunci:
$0 = y + (-y) = (y + y) + (-y) = y + (y + (-y)) = y + 0 = y = x0$
şi analog, $0x = 0$.

2. *Într-un inel A cu cel puţin două elemente* avem $1 \neq 0$.
În adevăr, dacă $1 = 0$, atunci $x = 1x = 0x = 0$, de unde $A = \{0\}$. Contradicţie!

3. (regula semnelor). *Oricare ar fi $x, y \in A$ avem*: $(-x)y = x(-y) = -xy$ şi $(-x)(-y) = xy$.
În adevăr, $0 = 0y = ((-x) + x)y = (-x)y + xy = xy + (-x)y$, de unde rezultă că $(-x)y$ este opusul lui xy, deci $(-x)y = -xy$. Analog, $x(-y) = -xy$. În fine, $(-x)(-y) = -(x(-y)) = -(-xy) = xy$.

4. (distributivitatea înmulţirii faţă de scădere). *Oricare ar fi $x, y, z \in A$, avem*: $x(y - z) = xy - xz$ şi $(y - z)x = yx - zx$.
Reamintim că $y + (-z)$ se notează cu $y - z$. Avem:

$$x(y - z) = x(y + (-z)) = xy + x(-z) = xy - xz$$

şi analog $(y - z)x = yx - zx$.

5. *Într-un inel A fără divizori ai lui zero, din $xy = xz$ sau $yx = zx$, cu $x \neq 0$, rezultă $y = z$.*

În adevăr, dacă $xy = xz$, atunci

$$x(y - z) = xy - xz = xy - xy = 0$$

şi cum $x \neq 0$ rezultă că $y - z = 0$, deci $y = z$. Analog, din $yx = zx$ rezultă $y = z$.

Exerciţii rezolvate

R — 1 Arătaţi că într-un inel comutativ A avem:

1) $(a + b)(a - b) = a^2 - b^2, \quad \forall a, b \in A$

2) $(a + b)^2 = a^2 + 2ab + b^2, \quad \forall a, b \in A,$

unde $2ab = ab + ab$ (v. Cap. III, § 1).

Soluţie. Folosind distributivitatea înmulţirii faţă de adunare şi apoi faţă de scădere avem:

$$(a + b)(a - b) = a(a - b) + b(a - b) = aa - ab + ba - bb =$$
$$= a^2 - ab + ab - b^2 = a^2 - b^2.$$

2) Conform definiţiei puterilor unui element şi distributivităţii înmulţirii faţă de adunare, avem:

$$(a + b)^2 = (a + b)(a + b) = (a + b)a + (a + b)b = a^2 + ba + ab + b^2 =$$
$$= a^2 + ab + ab + b^2 = a^2 + 2ab + b^2.$$

R — 2 Fie A un inel comutativ cu proprietatea:

$(\alpha) \qquad a + a + a = 0, \quad \forall a \in A.$

1) Arătaţi că $(a + b)^3 = a^3 + b^3, \quad \forall a, b \in A$;

2) Arătaţi că inelele $\mathcal{R}_3$ şi $M_2(\mathcal{R}_3)$ au proprietatea (α).

Soluţie. 1) Să arătăm la început că într-un inel comutativ este adevărată formula

$$(a + b)^3 = a^3 + 3a^2b + 3ab^2 + b^3, \quad \forall a, b \in A.$$

În adevăr, folosind rezultatul de la exerciţiul precedent, avem:

$$(a + b)^3 = (a + b)^2(a + b) = (a^2 + 2ab + b^2)(a + b) =$$
$$= (a^2 + 2ab + b^2)a + (a^2 + 2ab + b^2)b = a^3 + 2a^2b + b^2a + a^2b + 2ab^2 + b^3 =$$
$$= a^3 + 3a^2b + 3ab^2 + b^3.$$

Dar

$$3a^2b = a^2b + a^2b + a^2b = 0$$

şi analog $3ab^2 = 0$, de unde $(a + b)^3 = a^3 + b^3$.

2) În inelul $\mathcal{R}_3$ avem :

$$0\oplus0\oplus0 = (0\oplus0)\oplus0 = 0\oplus0 = 0,$$
$$1\oplus1\oplus1 = (1\oplus1)\oplus1 = 2\oplus1 = 0,$$
$$2\oplus2\oplus2 = (2\oplus2)\oplus2 = 1\oplus2 = 0,$$

de unde $a\oplus a\oplus a = 0$, $\forall\, a \in \mathcal{R}_3$.

Fie $U \in M_2(\mathcal{R}_3)$, $U = \begin{pmatrix} a & c \\ b & d \end{pmatrix}$ cu $a, b, c, d \in \mathcal{R}_3$.

În inelul $M_2(\mathcal{R}_3)$ avem :

$$U\oplus U\oplus U = \begin{pmatrix} a\oplus a\oplus a & b\oplus b\oplus b \\ c\oplus c\oplus c & d\oplus d\oplus d \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} = 0.$$

§ 3. INELUL CLASELOR DE RESTURI MODULO n

Fie $n > 0$ un număr întreg. Conform teoremei împărţirii cu rest, pentru orice $a \in \mathbf{Z}$ există $q, r \in \mathbf{Z}$ unic determinaţi astfel încît

$$a = nq + r, \quad 0 \leqslant r < n.$$

Numărul unic determinat r din relaţia precedentă, numit *restul* împărţirii lui a prin n, s-a notat cu a mod n şi s-a numit încă *redusul* modulo n al lui a (v. Cap. II, § 1).

Ca rezultat al împărţirii numerelor întregi prin $n > 0$ sînt posibile resturile :

$$0, 1, \ldots, r, \ldots, n-1.$$

Prin împărţirea lui a la n se obţine restul r dacă şi numai dacă a este de forma $nh + r$, cu $h \in \mathbf{Z}$. Mulţimile de numere

$$C_0, C_1, \ldots, C_r, \ldots, C_{n-1},$$

unde

$$C_0 = \{a \in \mathbf{Z} \mid a \bmod n = 0\} = \{nh \mid h \in \mathbf{Z}\} = n\mathbf{Z}$$
$$C_1 = \{a \in \mathbf{Z} \mid a \bmod n = 1\} = \{nh + 1 \mid h \in \mathbf{Z}\} = n\mathbf{Z} + 1$$
$$\vdots$$
$$C_r = \{a \in \mathbf{Z} \mid a \bmod n = r\} = \{nh + r \mid h \in \mathbf{Z}\} = n\mathbf{Z} + r$$
$$\vdots$$
$$C_{n-1} = \{a \in \mathbf{Z} \mid a \bmod n = n-1\} = \{nh + n - 1 \mid h \in \mathbf{Z}\} = n\mathbf{Z} + n - 1$$

se numesc *clase de resturi* modulo n.

Aşadar, un număr întreg a aparţine clasei C_r dacă şi numai dacă a împărţit la n dă restul r,

$$a \in C_r \Leftrightarrow a \bmod n = r.$$

În particular $r \in C_r$ pentru $r = 0, 1, \ldots, n-1$. Clasa de resturi C_r se notează de regulă cu $\hat{r}$. Aşadar

$$\hat{r} = C_r = n\mathbf{Z} + r,\ r \in \{0, 1, \ldots, n-1\}.$$

Să notăm cu $\mathbf{Z}_n$ mulţimea claselor de resturi modulo n,

$$\mathbf{Z}_n = \{\hat{0}, \hat{1}, \hat{2}, \ldots, \widehat{n-1}\}.$$

Dacă $\hat{a}, \hat{b} \in \mathbf{Z}_n$, definim *suma* $\hat{a} + \hat{b}$ şi *produsul* $\hat{a}\,\hat{b}$ prin :

$$\hat{a} + \hat{b} \stackrel{\text{def}}{=} \widehat{a \oplus b}, \quad \hat{a}\hat{b} \stackrel{\text{def}}{=} \widehat{a \otimes b}.$$

Se definesc astfel pe $\mathbf{Z}_n$, două legi de compoziţie :

$$\mathbf{Z}_n \times \mathbf{Z}_n \to \mathbf{Z}_n,\ (\hat{a}, \hat{b}) \to \hat{a} + \hat{b}$$

şi

$$\mathbf{Z}_n \times \mathbf{Z}_n \to \mathbf{Z}_n,\ (\hat{a}, \hat{b}) \to \hat{a}\,\hat{b},$$

numite *adunarea*, respectiv *înmulţirea* claselor de resturi modulo n.

Astfel, pentru $n = 6$ avem $\mathbf{Z}_6 = \{\hat{0}, \hat{1}, \hat{2}, \hat{3}, \hat{4}, \hat{5}\}$ şi tablele adunării şi înmulţirii claselor de resturi modulo 6 sînt :

$+$	$\hat{0}$	$\hat{1}$	$\hat{2}$	$\hat{3}$	$\hat{4}$	$\hat{5}$
$\hat{0}$	$\hat{0}$	$\hat{1}$	$\hat{2}$	$\hat{3}$	$\hat{4}$	$\hat{5}$
$\hat{1}$	$\hat{1}$	$\hat{2}$	$\hat{3}$	$\hat{4}$	$\hat{5}$	$\hat{0}$
$\hat{2}$	$\hat{2}$	$\hat{3}$	$\hat{4}$	$\hat{5}$	$\hat{0}$	$\hat{1}$
$\hat{3}$	$\hat{3}$	$\hat{4}$	$\hat{5}$	$\hat{0}$	$\hat{1}$	$\hat{2}$
$\hat{4}$	$\hat{4}$	$\hat{5}$	$\hat{0}$	$\hat{1}$	$\hat{2}$	$\hat{3}$
$\hat{5}$	$\hat{5}$	$\hat{0}$	$\hat{1}$	$\hat{2}$	$\hat{3}$	$\hat{4}$

$\cdot$	$\hat{0}$	$\hat{1}$	$\hat{2}$	$\hat{3}$	$\hat{4}$	$\hat{5}$
$\hat{0}$	$\hat{0}$	$\hat{0}$	$\hat{0}$	$\hat{0}$	$\hat{0}$	$\hat{0}$
$\hat{1}$	$\hat{0}$	$\hat{1}$	$\hat{2}$	$\hat{3}$	$\hat{4}$	$\hat{5}$
$\hat{2}$	$\hat{0}$	$\hat{2}$	$\hat{4}$	$\hat{0}$	$\hat{2}$	$\hat{4}$
$\hat{3}$	$\hat{0}$	$\hat{3}$	$\hat{0}$	$\hat{3}$	$\hat{0}$	$\hat{3}$
$\hat{4}$	$\hat{0}$	$\hat{4}$	$\hat{2}$	$\hat{0}$	$\hat{4}$	$\hat{2}$
$\hat{5}$	$\hat{0}$	$\hat{5}$	$\hat{4}$	$\hat{3}$	$\hat{2}$	$\hat{1}$

3.3. Teoremă. Adunarea şi înmulţirea claselor de resturi modulo n conferă mulţimii Z_n o structură de inel comutativ, numit ***inelul claselor de resturi modulo n.***

Demonstraţie. Să verificăm axiomele inelului comutativ. În esenţă demonstraţia se fundamentează pe faptul că $\mathcal{R}_n = \{0, 1, 2, \ldots, n-1\}$ are o structură de inel comutativ în raport cu operaţiile induse pe $\mathcal{R}_n$ de adunarea şi înmulţirea modulo n (v. ex. 3, § 1). De exemplu, axioma D se verifică astfel :

$$\hat{a}(\hat{b} + \hat{c}) = \hat{a}\widehat{b \oplus c} = \widehat{a \otimes (b \oplus c)} = \widehat{a \otimes b \oplus a \otimes c} = \widehat{a \otimes b} + \widehat{a \otimes c} =$$
$$= \hat{a}\,\hat{b} + \hat{a}\,\hat{c}$$

şi la fel se arată că G_1, G_4, M_1 şi M_3 sînt verificate de adunarea şi înmulţirea claselor de resturi modulo n.

Cum

$$\hat{0} + \hat{a} = \widehat{0 \oplus a} = \hat{a},\ \hat{1}\,\hat{a} = \widehat{1 \otimes a} = \hat{a},\ \forall \hat{a} \in \mathbf{Z}_n,$$

rezultă că şi axiomele G_2 şi M_2 sînt verificate

În fine, avem

$$\hat{a} + \widehat{n - a} = \widehat{a \oplus (n - a)} = \hat{0}, \quad \forall \hat{a} \in \mathbf{Z}_n, \text{ cu } a \neq 0$$

deci orice clasă $\hat{a} \in \mathbf{Z}_n$ este simetrizabilă în raport cu adunarea claselor de resturi modulo n

$$-\hat{a} = \widehat{n - a},\ \forall \hat{a} \in \mathbf{Z}_n,\ a \neq 0 \text{ și } -\hat{0} = \hat{0}.$$

3.4. *Remarcă.* Clasele de resturi modulo n au fost notate cu $\hat{0}, \hat{1}, \ldots, \widehat{n - 1}$. Numerele $0, 1, \ldots, n - 1$ se numesc *reprezentanții canonici* ai claselor de resturi $\hat{0}, \hat{1}, \ldots, \widehat{n - 1}$ respectiv.

În aplicații este adesea preferabil să descriem clasele de resturi și cu alte numere care aparțin acestora. În acest sens, pentru orice $x \in \mathbf{Z}$, se notează cu $\hat{x}$ clasa de resturi C_r, $0 \leqslant r < n$ astfel încît $x \in C_r$; $\hat{x}$ se numește *clasa* lui x modulo n.

Așadar, prin definiție avem :

(α) $$\hat{x} \overset{\text{def}}{=\!=} \widehat{x \bmod n}, \quad \forall x \in \mathbf{Z}.$$

Astfel, dacă $n = 5$, atunci

$$\widehat{32} = \widehat{32 \bmod 5} = \widehat{(6 \cdot 5 + 2) \bmod 5} = 6 \cdot 5 \bmod 5 + \widehat{2 \bmod 5} = \hat{2} \in \mathbf{Z}_5,$$

$$\widehat{-7} = \widehat{(-7) \bmod 5} = \widehat{(-2) \bmod 5} = \widehat{(0-2) \bmod 5} = \widehat{(5-2) \bmod 5} = \hat{3} \in Z_5,$$

$$\widehat{25} = \widehat{25 \bmod 5} = \hat{0} \in \mathbf{Z}_5.$$

Spunem că numărul întreg x este *congruent* cu y modulo n, și scriem $x \equiv y \pmod n$ dacă și numai dacă $n \mid x - y$ sau altfel scris $\frac{x - y}{n} \in \mathbf{Z}$.

Din definiția (α) rezultă că pentru orice $x, y \in \mathbf{Z}$ avem :

(β) $$\hat{x} = \hat{y} \Leftrightarrow x \bmod n = y \bmod n \Leftrightarrow n \mid x - y \Leftrightarrow x \equiv y \pmod n.$$

Să mai observăm că operațiile cu clase de resturi date prin reprezentanți arbitrari se pot efectua după regulile :

(γ) $$\hat{x} + \hat{y} = \widehat{x + y}, \quad \hat{x}\,\hat{y} = \widehat{x\,y}, \quad \forall x, y \in Z_n.$$

În adevăr, fie $a = x \bmod n$, $b = y \bmod n$ și $h, k \in \mathbf{Z}$ astfel încît :

$$x = nh + a, \qquad y = nk + b.$$

Atunci

$$x + y = n(h + k) + (a + b), \qquad xy = n(nhk + ak + hb) + ab.$$

Cum $a \oplus b = (a + b) \bmod n$ şi $a \otimes b = (ab) \bmod n$, acum din (β) şi Teorema 8.1, Cap. II rezultă :

$$\hat{x} + \hat{y} = \hat{a} + \hat{b} = \widehat{a \oplus b} = \widehat{a + b} = \widehat{x + y}$$

şi

$$\hat{x}\hat{y} = \hat{a}\hat{b} = \widehat{a \otimes b} = \widehat{ab} = \widehat{xy}.$$

Exerciţii rezolvate

R — 1 Fie $M_2(\mathbf{Z}_6)$ inelul matricelor pătratice de ordin 2 cu coeficienţi din $\mathbf{Z}_6$ şi $U, V, E, X \in M_2(\mathbf{Z}_6)$,

$$U = \begin{pmatrix} \hat{3} & \hat{5} \\ \hat{5} & \hat{4} \end{pmatrix}, \quad V = \begin{pmatrix} \hat{3} & \hat{1} \\ \hat{1} & \hat{2} \end{pmatrix}, \quad E = \begin{pmatrix} \hat{1} & \hat{0} \\ \hat{0} & \hat{1} \end{pmatrix}, \quad X = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}.$$

1) Calculaţi $U + V$ şi UV;

2) Determinaţi pe X astfel încît $UX = E$. Deduceţi că U este element inversabil al inelului $M_2(\mathbf{Z}_6)$.

Soluţie. 1) Avem :

$$U + V = \begin{pmatrix} \hat{3} & \hat{5} \\ \hat{5} & \hat{4} \end{pmatrix} + \begin{pmatrix} \hat{3} & \hat{1} \\ \hat{1} & \hat{2} \end{pmatrix} = \begin{pmatrix} \hat{3} + \hat{3} & \hat{5} + \hat{1} \\ \hat{5} + \hat{1} & \hat{4} + \hat{2} \end{pmatrix} = \begin{pmatrix} \hat{0} & \hat{0} \\ \hat{0} & \hat{0} \end{pmatrix}$$

şi

$$UV = \begin{pmatrix} \hat{3} & \hat{5} \\ \hat{5} & \hat{4} \end{pmatrix} \begin{pmatrix} \hat{3} & \hat{1} \\ \hat{1} & \hat{2} \end{pmatrix} = \begin{pmatrix} \hat{3} \cdot \hat{3} + \hat{5} \cdot \hat{1} & \hat{3} \cdot \hat{1} + \hat{5} \cdot \hat{2} \\ \hat{5} \cdot \hat{3} + \hat{4} \cdot \hat{1} & \hat{5} \cdot \hat{1} + \hat{4} \cdot \hat{2} \end{pmatrix} = \begin{pmatrix} \hat{2} & \hat{1} \\ \hat{1} & \hat{1} \end{pmatrix}.$$

2) Avem

$$\begin{pmatrix} \hat{1} & \hat{0} \\ \hat{0} & \hat{1} \end{pmatrix} = E = UX = \begin{pmatrix} \hat{3}\alpha + \hat{5}\gamma & \hat{3}\beta + \hat{5}\delta \\ \hat{5}\alpha + \hat{4}\gamma & \hat{5}\beta + \hat{4}\delta \end{pmatrix}$$

ceea ce revine la :

$$\text{a)} \begin{cases} \hat{3}\alpha + \hat{5}\gamma = \hat{1} \\ \hat{5}\alpha + \hat{4}\gamma = \hat{0} \end{cases} \quad \text{şi b)} \begin{cases} \hat{3}\beta + \hat{5}\delta = \hat{0} \\ \hat{5}\beta + \hat{4}\delta = \hat{1}. \end{cases}$$

Să rezolvăm sistemul a). Să observăm că elementele inversabile ale inelului $\mathbf{Z}_6$ sînt $\hat{1}$ şi $\hat{5}$ (v. tabla înmulţirii inelului $\mathbf{Z}_6$) şi că $(\hat{1})^{-1} = \hat{1}$, $(\hat{5})^{-1} = \hat{5}$. Necunoscutele sistemului care au ca coeficienţi elemente inversabile din $\mathbf{Z}_6$ pot fi exprimate în funcţie de celelalte. Astfel, este posibil să facem aceasta cu necunoscuta α din a doua ecuaţie. Cum $\gamma \in \mathbf{Z}_6$, în inelul $\mathbf{Z}_6$ putem face calculul :

$$\hat{4}\gamma + \hat{2}\gamma = (\hat{4} + \hat{2})\gamma = \hat{0}\gamma = \hat{0}.$$

Aşadar, adunînd pe $\hat{2}\gamma$ la fiecare termen al ecuaţiei a doua se obţine

$$\hat{5}\alpha = \hat{2}\gamma$$

de unde, prin înmulţire cu $(\hat{5})^{-1} = \hat{5}$ deducem

$$\hat{5}\,(\hat{5}\alpha) = \hat{5}\,(\hat{2}\gamma)$$

deci

$$(\hat{5}\cdot\hat{5})\alpha = (\hat{5}\cdot\hat{2})\gamma$$

şi în definitiv $\alpha = \hat{4}\gamma$. Înlocuind în prima ecuaţie pe α cu $\hat{4}\gamma$ aceasta devine

$$\hat{5}\gamma = \hat{1}$$

deci $\gamma = \hat{5}$ şi atunci $\alpha = \hat{4}\gamma = \hat{4}\cdot\hat{5} = \hat{2}$.

Analog se rezolvă sistemul b) şi se obţine $\beta = \hat{5}$, $\delta = \hat{3}$, deci

$$X = \begin{pmatrix} \hat{2} & \hat{5} \\ \hat{5} & \hat{3} \end{pmatrix} \in M_2(\mathbf{Z}_6).$$

Cum

$$XU = \begin{pmatrix} \hat{2} & \hat{5} \\ \hat{5} & \hat{3} \end{pmatrix}\begin{pmatrix} \hat{3} & \hat{5} \\ \hat{5} & \hat{4} \end{pmatrix} = \begin{pmatrix} \hat{2}\cdot\hat{3}+\hat{5}\cdot\hat{5} & \hat{2}\cdot\hat{5}+\hat{5}\cdot\hat{4} \\ \hat{5}\cdot\hat{3}+\hat{3}\cdot\hat{5} & \hat{5}\cdot\hat{5}+\hat{3}\cdot\hat{4} \end{pmatrix} = \begin{pmatrix} \hat{1} & \hat{0} \\ \hat{0} & \hat{1} \end{pmatrix}$$

avem $XU = E$. Analog $UX = E$, deci U este element inversabil al inelului $M_2(\mathbf{Z}_6)$ şi

$$U^{-1} = \begin{pmatrix} \hat{2} & \hat{5} \\ \hat{5} & \hat{3} \end{pmatrix}.$$

R — 2 1) Fie $\hat{a} \in \mathbf{Z}_n$. Arătaţi că $\hat{a}$ este element inversabil al inelului $\mathbf{Z}_n$ dacă şi numai dacă a este relativ prim cu n;

2) Determinaţi elementele inversabile ale inelului $\mathbf{Z}_9$ şi rezolvaţi în inelul $\mathbf{Z}_9$ ecuaţia $\hat{7}x + \hat{3} = \hat{2}$.

Soluţie. 1) Presupunem că $\hat{a}$ este inversabilă în inelul $\mathbf{Z}_n$. Atunci există $\hat{b} \in \mathbf{Z}_n$ astfel încît $\hat{a}\,\hat{b} = \hat{1}$. Cum

$$\widehat{ab} = \hat{a}\,\hat{b} = \hat{1}$$

avem $\widehat{ab} = \hat{1}$ şi din proprietatea (β) rezultă că numărul $ab - 1$ se divide prin n. Există deci $k \in \mathbf{Z}$ astfel încît $ab - 1 = nk$. Asadar

$$a\cdot b + n(-k) = 1,$$

de unde $(a, n) = 1$, (v. § 4, Cap. I).

Reciproc, dacă $(a, n) = 1$, există $h, k \in \mathbf{Z}$ astfel încît $ah + nk = 1$ (v. § 4, Cap. I).

Cum
$$\hat{1} = \widehat{ah + nk} = \widehat{ah} + \widehat{nk} = \widehat{ah} + \hat{0} = \hat{a}\hat{h}$$

rezultă că $\hat{a}$ este element inversabil al inelului $\mathbf{Z}_n$ şi $(\hat{a})^{-1} = \hat{h}$.

2) Elementele inelului $\mathbf{Z}_9$ sînt $\hat{0}, \hat{1}, \hat{2}, \ldots, \hat{8}$.
Dintre numerele 0, 1, 2, ..., 8 sînt relativ prime cu 9 numerele 1, 2, 4, 5, 7 şi 8, deci elementele inversabile ale inelului $\mathbf{Z}_9$ sînt $\hat{1}, \hat{2}, \hat{4}, \hat{5}, \hat{7}$ şi $\hat{8}$. Din tabla înmulţirii inelului $\mathbf{Z}_9$ se pot determina inversele acestor clase.

Se constată că : $(\hat{1})^{-1} = \hat{1}$, $(\hat{2})^{-1} = \hat{5}$, $(\hat{4})^{-1} = \hat{7}$, $(\hat{5})^{-1} = \hat{2}$ şi $(\hat{7})^{-1} = \hat{4}$.

Ecuaţia dată se rezolvă astfel :

$$\hat{7}x = \hat{2} + (-\hat{3}) = \hat{2} + \widehat{0 - 3} = \hat{2} + \widehat{9 - 3} = \hat{2} + \hat{6} = \widehat{2 + 6} = \hat{8}$$

şi atunci

$$x = (\hat{7})^{-1}\hat{8} = \hat{4}\cdot\hat{8} = \widehat{4\cdot 8} = \widehat{32} = \widehat{3\cdot 9 + 5} = \hat{3}\cdot\hat{9} + \hat{5} = \hat{3}\cdot\hat{0} + \hat{5} = \hat{5}.$$

Pentru a determina inversele acestor clase mai putem proceda :

fie $\hat{2}^{-1} = \hat{a} \in \mathbf{Z}_9 \Leftrightarrow 2a \equiv 1 \pmod 9 \Leftrightarrow \dfrac{2a - 1}{9} \in \mathbf{Z} \Leftrightarrow a \equiv 5 \pmod 9$, deci $\hat{2}^{-1} = \hat{5}$;

fie $\hat{4}^{-1} = \hat{b} \in \mathbf{Z}_9 \Leftrightarrow 4b \equiv 1 \pmod 9 \Leftrightarrow \dfrac{4b - 1}{9} \in \mathbf{Z} \Leftrightarrow b \equiv 7 \pmod 9$, deci $\hat{4}^{-1} = \hat{7}$;

fie $\hat{5}^{-1} = \hat{c} \in \mathbf{Z}_9 \Leftrightarrow 5c \equiv 1 \pmod 9 \Leftrightarrow \dfrac{5c - 1}{9} \in \mathbf{Z} \Leftrightarrow c \equiv 2 \pmod 9$, deci $\hat{5}^{-1} = \hat{2}$;

fie $\hat{7}^{-1} = \hat{d} \in \mathbf{Z}_9 \Leftrightarrow 7d \equiv 1 \pmod 9 \Leftrightarrow \dfrac{7d - 1}{9} \in \mathbf{Z} \Leftrightarrow d \equiv 4 \pmod 9$, deci $\hat{7}^{-1} = \hat{4}$.

Un cadru ideal pentru perfectarea calculelor algebrice este dat de inelele cu proprietatea că orice element diferit de 0 este simetrizabil în raport cu înmulţirea. Asemenea inele sînt cunoscute sub numele de *corpuri*. Mai precis :

4.1. *Definiţie.* **Un inel K se numeşte *corp* dacă $0 \neq 1$ şi orice element $x \in K$, $x \neq 0$, este simetrizabil în raport cu înmulţirea :**

$$\forall x \in K,\ x \neq 0 \Rightarrow \exists x^{-1} \in K \text{ astfel încît } x^{-1}x = xx^{-1} = 1.$$

Un corp K se numeşte *comutativ* dacă înmulţirea sa este comutativă.

Proprietăţi

1. *Corpurile nu au divizori ai lui zero.* În adevăr, dacă $x, y \in K$, $x \neq 0$ şi $y \neq 0$, atunci $xy \neq 0$ căci dacă $xy = 0$ deducem

$$y = 1\cdot y = (x^{-1}x)y = x^{-1}(xy) = x^{-1}0 = 0,$$

deci $y = 0$. Contradicţie.

2. *Elementele diferite de zero dintr-un corp formează grup faţă de înmulţire.* În adevăr, fie K un corp şi $K^* = K \setminus \{0\}$. Din proprietatea 1) rezultă că K^* este o parte stabilă a lui K în raport cu înmulţirea. Cum $1 \neq 0$, rezultă că $1 \in K^*$. Deducem că operaţia indusă pe K^* de înmulţirea lui K este asociativă şi admite pe 1 ca element neutru Fie $x \in K^*$. Atunci $x \neq 0$ şi fie x^{-1} inversul său în raport cu înmulţirea lui K. Cum $x^{-1}x = 1 \neq 0$, rezultă că $x^{-1} \neq 0$, deci $x^{-1} \in K^*$. Evident, x^{-1} este inversul lui x şi în raport cu operaţia indusă. Deci $(K^*, \cdot)$ este grup, numit *grupul multiplicativ* al corpului K.

Exemple

1. *Corpurile* $\mathbf{Q}$, $\mathbf{R}$ *și* $\mathbf{C}$. Din proprietățile adunării și înmulțirii numerelor (v. § 1, Cap. I) rezultă că $(\mathbf{Q}, +, \cdot)$, $(\mathbf{R}, +, \cdot)$ și $(\mathbf{C}, +, \cdot)$ sînt corpuri comutative, numite respectiv *corpul numerelor raționale, corpul numerelor reale, corpul numerelor complexe.*
2. *Corpurile de numere pătratice* $\mathbf{Q}(\sqrt{d})$. Fie d un întreg liber de pătrate și

$$\mathbf{Q}(\sqrt{d}) = \{a + b\sqrt{d} \mid a,\ b \in \mathbf{Q}\}.$$

Dacă $z,\ w \in \mathbf{Q}(\sqrt{d})$, $z = a + b\sqrt{d}$, $w = u + v\sqrt{d}$ cu $a,\ b,\ u,\ v \in \mathbf{Q}$, atunci

$$z + w = (a + u) + (b + v)\sqrt{d} \in \mathbf{Q}(\sqrt{d}),$$

$$zw = (au + dbv) + (av + bu)\sqrt{d} \in \mathbf{Q}(\sqrt{d})$$

deci $\mathbf{Q}(\sqrt{d})$ este o parte stabilă a lui $\mathbf{C}$ în raport cu adunarea și înmulțirea. Observînd că $0 = 0 + 0 \cdot \sqrt{d} \in \mathbf{Q}(\sqrt{d})$, $1 = 1 + 0 \cdot \sqrt{d} \in \mathbf{Q}(\sqrt{d})$ se deduce ușor că $\mathbf{Q}(\sqrt{d})$ este inel comutativ în raport cu operațiile induse pe $\mathbf{Q}(\sqrt{d})$ de adunarea și înmulțirea lui $\mathbf{C}$. Pentru a dovedi că $\mathbf{Q}(\sqrt{d})$ este corp mai rămîne să arătăm că pentru orice $z \in \mathbf{Q}(\sqrt{d})$, $z = a + b\sqrt{d}$, $z \neq 0$, există $z' \in \mathbf{Q}(\sqrt{d})$ astfel încît $zz' = 1$.

Dacă $z \neq 0$, atunci $a \neq 0$ sau $b \neq 0$. Rezultă că $a^2 - db^2 \neq 0$ (dacă $a^2 - db^2 = 0$ și $b = 0$ deducem și $a = 0$, iar dacă $a^2 - db^2 = 0$ și $b \neq 0$ deducem $\sqrt{d} \in \mathbf{Q}$, ambele situații fiind contradictorii.

Fie

$$z' = \frac{a}{a^2 - db^2} - \frac{b}{a^2 - db^2}\sqrt{d} \in \mathbf{Q}(\sqrt{d})$$

și avem :

$$zz' = 1.$$

Rezultă că $\mathbf{Q}(\sqrt{d})$ formează corp față de operațiile induse de adunarea și înmulțirea din $\mathbf{C}$, numit *corp de numere pătratice*. Astfel $\mathbf{Q}(\sqrt{2})$, $\mathbf{Q}(i)$, $\mathbf{Q}(\sqrt{-5})$ etc. sînt corpuri de numere pătratice.
3. Inelele $(\mathbf{Z}, +, \cdot)$ și $(\mathbf{Z}_6, +, \cdot)$ nu sînt corpuri. În adevăr, $2x \neq 1$ oricare ar fi $x \in \mathbf{Z}$, deci 2 nu este inversabil în raport cu înmulțirea lui $\mathbf{Z}$. În inelul $\mathbf{Z}_6$ avem $\hat{3} \cdot \hat{4} = 0$ și cum corpurile nu au divizori ai lui zero rezultă că $(\mathbf{Z}_6, +, \cdot)$ nu este corp.
4. *Corpul* $\mathbf{Z}_p$ *al claselor de resturi modulo* p. Fie $p > 0$ un număr prim. Atunci inelul $\mathbf{Z}_p$ este corp.
În adevăr, elementele lui $\mathbf{Z}_p$ sînt

$$\hat{0},\ \hat{1},\ \hat{2}, \ldots,\ \widehat{p - 1}.$$

Pentru orice $a \in \mathbf{Z}$, $1 \leqslant a < p$ avem $(a, p) = 1$.
În adevăr, p fiind prim, singurii divizori pozitivi ai lui p sînt 1 și p.

Cum $1 \leqslant a < p$, p nu divide pe a, deci a şi p admit un singur divizor comun pozitiv, anume pe 1. Atunci şi c.m.m.d.c. al lui a şi p este egal cu 1, deci $(a, p) = 1$. Aplicînd acum rezultatul de la Ex. R—2, § 3, deducem că orice clasă $\hat{a} \in \mathbf{Z}_p$, $\hat{a} \neq \hat{0}$, este inversabilă în raport cu înmulţirea, deci $\mathbf{Z}_p$ este corp. În particular $\mathbf{Z}_5$ este corp. Faptul că orice clasă $\hat{a} \in \mathbf{Z}_5$, $\hat{a} \neq \hat{0}$, este inversabilă în raport cu înmulţirea se observă şi pe tabla înmulţirii lui $\mathbf{Z}_5$: $(\hat{1})^{-1} = \hat{1}$, $(\hat{2})^{-1} = \hat{3}$, $(\hat{3})^{-1} = \hat{2}$, $(\hat{4})^{-1} = \hat{4}$.

$+$	$\hat{0}$	$\hat{1}$	$\hat{2}$	$\hat{3}$	$\hat{4}$
$\hat{0}$	$\hat{0}$	$\hat{1}$	$\hat{2}$	$\hat{3}$	$\hat{4}$
$\hat{1}$	$\hat{1}$	$\hat{2}$	$\hat{3}$	$\hat{4}$	$\hat{0}$
$\hat{2}$	$\hat{2}$	$\hat{3}$	$\hat{4}$	$\hat{0}$	$\hat{1}$
$\hat{3}$	$\hat{3}$	$\hat{4}$	$\hat{0}$	$\hat{1}$	$\hat{2}$
$\hat{4}$	$\hat{4}$	$\hat{0}$	$\hat{1}$	$\hat{2}$	$\hat{3}$

Tabla adunării lui $\mathbf{Z}_5$.

$\cdot$	$\hat{0}$	$\hat{1}$	$\hat{2}$	$\hat{3}$	$\hat{4}$
$\hat{0}$	$\hat{0}$	$\hat{0}$	$\hat{0}$	$\hat{0}$	$\hat{0}$
$\hat{1}$	$\hat{0}$	$\hat{1}$	$\hat{2}$	$\hat{3}$	$\hat{4}$
$\hat{2}$	$\hat{0}$	$\hat{2}$	$\hat{4}$	$\hat{1}$	$\hat{3}$
$\hat{3}$	$\hat{0}$	$\hat{3}$	$\hat{1}$	$\hat{4}$	$\hat{2}$
$\hat{4}$	$\hat{0}$	$\hat{4}$	$\hat{3}$	$\hat{2}$	$\hat{1}$

Tabla înmulţirii lui $\mathbf{Z}_5$.

Exerciţii rezolvate

R — 1 *Un corp cu patru elemente*. Fie $K = \{0, 1, a, b\}$ unde $0, 1, a, b \in M_2(\mathbf{Z}_2)$,

$$0 = \begin{pmatrix} \hat{0} & \hat{0} \\ \hat{0} & \hat{0} \end{pmatrix},\ 1 = \begin{pmatrix} \hat{1} & \hat{0} \\ \hat{0} & \hat{1} \end{pmatrix},\ a = \begin{pmatrix} \hat{0} & \hat{1} \\ \hat{1} & \hat{1} \end{pmatrix},\ b = \begin{pmatrix} \hat{1} & \hat{1} \\ \hat{1} & \hat{0} \end{pmatrix}.$$

Arătaţi:

1. K este o parte stabilă a lui $M_2(\mathbf{Z}_2)$ în raport cu adunarea şi înmulţirea matricelor şi alcătuiţi tablele operaţiilor induse.

2. Operaţiile induse conferă lui K o structură de corp comutativ.

Soluţie. 1) Conform definiţiei operaţiilor cu matrice, avem:

$$1 + a = \begin{pmatrix} \hat{1} & \hat{0} \\ \hat{0} & \hat{1} \end{pmatrix} + \begin{pmatrix} \hat{0} & \hat{1} \\ \hat{1} & \hat{1} \end{pmatrix} = \begin{pmatrix} \hat{1} + \hat{0} & \hat{0} + \hat{1} \\ \hat{0} + \hat{1} & \hat{1} + \hat{1} \end{pmatrix} = \begin{pmatrix} \hat{1} & \hat{1} \\ \hat{1} & \hat{0} \end{pmatrix} = b \in K$$

$$ab = \begin{pmatrix} \hat{0} & \hat{1} \\ \hat{1} & \hat{1} \end{pmatrix}\begin{pmatrix} \hat{1} & \hat{1} \\ \hat{1} & \hat{0} \end{pmatrix} = \begin{pmatrix} \hat{0}\cdot\hat{1} + \hat{1}\cdot\hat{1} & \hat{0}\cdot\hat{1} + \hat{1}\cdot\hat{0} \\ \hat{1}\cdot\hat{1} + \hat{1}\cdot\hat{1} & \hat{1}\cdot\hat{1} + \hat{1}\cdot\hat{0} \end{pmatrix} = \begin{pmatrix} \hat{1} & \hat{0} \\ \hat{0} & \hat{1} \end{pmatrix} = 1 \in K$$

ş.a.m.d.

Aşadar K este o parte stabilă a lui $M_2(\mathbf{Z}_2)$ în raport cu operaţiile de adunare şi înmulţire, tablele operaţiilor induse fiind:

+	0	1	a	b
0	0	1	a	b
1	1	0	b	a
a	a	b	0	1
b	b	a	1	0

·	0	1	a	b
0	0	0	0	0
1	0	1	a	b
a	0	a	b	1
b	0	b	1	a

2) Cum adunarea şi înmulţirea matricelor sînt operaţii asociative, la fel vor fi şi operaţiile induse pe K. Din acelaşi motiv operaţia indusă de înmulţire este distributivă în raport cu operaţia indusă de adunare.

Pe tabla adunării lui K se observă că această operaţie este comutativă, admite pe 0 ca element neutru şi orice element din K are opus. Pe tabla înmulţirii lui K se observă că această operaţie este comutativă, admite pe 1 ca element neutru şi orice element din K diferit de 0 are invers. Aşadar $(K, +, \cdot)$ este corp comutativ.

R — 2 1) *Teorema lui Fermat*. Fie $a, p \in \mathbf{Z}$, cu $p > 0$ număr prim care nu divide pe a. Arătaţi că:

$$a^{p-1} \equiv 1 \pmod p.$$

2) Fie $a = 149^{128}$. Calculaţi $a \bmod 7$.

Soluţie. Fie $Z_p^* = Z_p \setminus \{\hat{0}\}$. Cum $(\mathbf{Z}_p^*, \cdot)$ este un grup comutativ, din Ex. R—2, Cap. III, § 3, rezultă:

$$(\hat{x})^{p-1} = \hat{1}, \qquad \forall \hat{x} \in \mathbf{Z}_p^*.$$

Dar cum p nu divide pe a rezultă că

$$a \bmod p \neq 0, \text{ deci}$$

$$\hat{a} = \widehat{a \bmod p} \neq \hat{0}.$$

Deducem că $\hat{a} \in \mathbf{Z}_p^*$, deci

$$\hat{1} = (\hat{a})^{p-1} = \widehat{a^{p-1}},$$

de unde $a^{p-1} \equiv 1 \pmod p$.

2) În corpul $\mathbf{Z}_7$, avem

$$\widehat{149} = \widehat{149 \bmod 7} = \widehat{(21 \cdot 7 + 2) \bmod 7} = \hat{2}.$$

Cum 7 nu divide pe 2, conform teoremei lui Fermat avem

$$2^6 \equiv 1 \pmod 7). \text{ Atunci în corpul } \mathbf{Z}_7 \text{ avem: } \hat{1} = \widehat{2^6} = (\hat{2})^6, \text{ deci } (\hat{2})^6 = \hat{1}.$$

Dar $128 = 6 \cdot 21 + 2$, deci

$$\widehat{149^{128}} = (\widehat{149})^{128} = (\hat{2})^{128} = (\hat{2})^{6 \cdot 21 + 2} = ((\hat{2})^6)^{21} \cdot (\hat{2})^2 = \widehat{2^2} = \hat{4},$$

de unde $a \bmod 7 = 4$.

§ 5. MORFISME DE INELE ŞI CORPURI

Ca şi în cazul grupurilor, noţiunea de izomorfism de inele (corpuri) constituie un criteriu de clasificare a inelelor (respectiv corpurilor), un criteriu de identificare a inelelor (respectiv corpurilor) cu aceleaşi proprietăţi algebrice.

5.1. *Definiţie.* **Fie A şi A' două inele. O aplicaţie bijectivă $f : A \to A'$ se numeşte** *izomorfism* **de inele dacă**

$$1)\ f(x + y) = f(x) + f(y),$$

$$2)\ f(xy) = f(x)f(y)$$

oricare ar fi, x, $y \in A$.

Vom spune că inelul A este izomorf cu inelul A', şi scriem $A \simeq A'$, dacă există cel puţin un izomorfism $f: A \to A'$.

Să observăm că dacă $f: A \to A'$ este un izomorfism de inele, atunci $f(1) = 1'$. În adevăr, acest lucru decurge din surjectivitatea lui f căci dacă $x' \in A'$ atunci $x' = f(x)$ cu $x \in A$, deci :

$$f(1)x' = f(1)f(x) = f(1 \cdot x) = f(x) = x' = x'f(1),$$

de unde $f(1) = 1'$.

Renunţînd la condiţia de bijectivitate asupra lui f în definiţia de mai sus şi adăugînd cerinţa :

$$3)\ f(1) = 1'$$

se obţine noţiunea de *morfism* (*omomorfism*) de inele.

Dacă $f: A \to A'$ este morfism de inele, atunci din 1) rezultă că f este morfism de la grupul $(A, +)$ la grupul $(A', +)$. Conform rezultatelor obţinute pentru morfisme de grupuri, rezultă că :

$$f(0) = 0'$$

$$f(-x) = -f(x) \qquad \forall x \in A.$$

Cu un argument asemănător celui folosit la grupuri, se arată că dacă $x \in A$ este inversabil, atunci $f(x)$ este element inversabil al lui A' şi

$$f(x^{-1}) = (f(x))^{-1}.$$

Vom spune că o aplicaţie $f: K \to K'$ de la un corp K la un corp K' este *izomorfism* (*morfism*) de corpuri dacă f este izomorfism (respectiv morfism) de inele de la K la K'.

Orice morfism de corpuri $f: K \to K'$ este injectiv. În adevăr, fie $x_1, x_2 \in K$ astfel încît $f(x_1) = f(x_2)$ şi să notăm $x = x_1 - x_2$.

Avem :

$$f(x) = f(x_1 + (-x_2)) = f(x_1) + f(-x_2) = f(x_1) + (-f(x_2)) = f(x_1) + (-f(x_1)) = 0'.$$

Dacă $x \neq 0$, atunci putem scrie

$$1' = f(1) = f(xx^{-1}) = f(x)f(x^{-1}) = 0'f(x^{-1}) = 0'.$$

Contradicţie, căci $1' \neq 0'$. Rămîne adevărat că $x = 0$, deci $x_1 = x_2$, de unde rezultă că f este injectiv.

Dacă A este un inel, atunci ca şi în cazul grupurilor, un izomorfism (morfism) $f : A \to A$ se numeşte *automorfism* (resp. *endomorfism*) al inelului A. Aceeaşi terminologie se foloseşte şi pentru corpuri.

Exemple

1. Aplicaţia $f : \mathbf{Z} \to M_2(\mathbf{Z})$,

$$f(a) = \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}, \ \forall a \in \mathbf{Z}$$

este un morfism injectiv de inele. În adevăr, pentru orice $a, b \in \mathbf{Z}$ avem :

$$f(a+b) = \begin{pmatrix} a+b & 0 \\ 0 & a+b \end{pmatrix} = \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} + \begin{pmatrix} b & 0 \\ 0 & b \end{pmatrix} = f(a) + f(b)$$

$$f(ab) = \begin{pmatrix} ab & 0 \\ 0 & ab \end{pmatrix} = \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}\begin{pmatrix} b & 0 \\ 0 & b \end{pmatrix} = f(a)f(b)$$

$$f(1) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Injectivitatea lui f este evidentă.

2. Pentru orice $z \in \mathbf{C}$, $z = a + bi$ cu $a, b \in \mathbf{R}$, notăm cu $\bar{z} = a - bi$ *conjugatul* lui z. Aplicaţia

$$f : \mathbf{C} \to \mathbf{C}, \quad f(z) = \bar{z}, \quad \forall z \in \mathbf{C}$$

este un automofism al corpului $\mathbf{C}$. În adevăr

$$f(z + w) = \overline{z + w} = \bar{z} + \bar{w} = f(z) + f(w),$$

$$f(zw) = \overline{zw} = \bar{z}\bar{w} = f(z)f(w)$$

oricare ar fi $z, w \in \mathbf{C}$.

Cum $z = \bar{\bar{z}} = f(\bar{z})$, rezultă că f este surjectiv şi cum orice morfism de corpuri este injectiv, deducem că f este automorfism al corpului $\mathbf{C}$.

Exerciţii rezolvate

R − 1 Fie $K = \{0, 1, a, b\}$ corpul cu patru elemente de la Ex. R − 1, §4.

Arătaţi că :

1) $(x + y)^2 = x^2 + y^2$, $(xy)^2 = x^2y^2$, $\forall x, y \in K$.

2) Aplicația $f: K \to K$, $f(x) = x^2$, $\forall x \in K$ este automorfism al corpului K și $f \neq 1_K$.

3) Dacă $g \neq 1_K$ este automorfism al lui K, atunci $g = f$.

Soluție. 1) Din tabla adunării corpului K (v. § 4) rezultă că :

$$2x = x + x = 0, \quad \forall x \in K.$$

Cum corpul K este comutativ, pentru orice $x, y \in K$, avem :

$$(x + y)^2 = (x + y)(x + y) = x(x + y) + y(x + y) = x^2 + xy + yx + y^2 =$$
$$= x^2 + xy + xy + y^2 = x^2 + (x + x)y + y^2 = x^2 + 0y + y^2 = x^2 + y^2$$

și

$$(xy)^2 = (xy)(xy) = x(y(xy)) = x((yx)y) = x((xy)y) = x(x(yy)) = x(xy^2) = (xx)y^2 = x^2y^2.$$

2) Folosind pct. 1, pentru orice $x, y \in K$, avem :

$$f(x + y) = (x + y)^2 = x^2 + y^2 = f(x) + f(y)$$

și

$$f(xy) = (xy)^2 = x^2y^2 = f(x)f(y).$$

Rămîne să arătăm că f este bijectiv. Folosind tabla înmulțirii corpului K (v. § 4) valorile aplicației f pot fi date prin tabelul următor :

x	0	1	a	b
$f(x) = x^2$	0	1	b	a

Se observă astfel că $f \neq 1_K$ și că f este aplicație bijectivă.

3) Cum g este morfism de corpuri avem $g(0) = 0$ și $g(1) = 1$. Atunci, pentru ca $g \neq 1_K$ trebuie ca $g(a) = b$ și $g(b) = a$, de unde $g = f$.

R — 2 Fie K mulțimea tuturor matricelor $U \in M_2(\mathbb{R})$ de forma

$$U = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}, \quad a, \ b \in \mathbb{R}.$$

1) Arătați că mulțimea K este o parte stabilă a lui $M_2(\mathbb{R})$ în raport cu adunarea și înmulțirea matricelor și că operațiile induse conferă lui K o structură de corp.

2) $\mathbb{C} \simeq K$.

Soluție. 1) Fie $U, V \in K$,

$$U = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}, \quad V = \begin{pmatrix} c & d \\ -d & c \end{pmatrix}.$$

Avem :

$$U + V = \begin{pmatrix} a & b \\ -b & a \end{pmatrix} + \begin{pmatrix} c & d \\ -d & c \end{pmatrix} = \begin{pmatrix} a + c & b + d \\ -(b + d) & a + c \end{pmatrix} \in K$$

și

$$UV = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}\begin{pmatrix} c & d \\ -d & c \end{pmatrix} = \begin{pmatrix} ac - bd & ad + bc \\ -(ad + bc) & ac - bd \end{pmatrix} \in K.$$

Se mai observă că

$$0=\begin{pmatrix}0 & 0\\0 & 0\end{pmatrix}\in K,\ E=\begin{pmatrix}1 & 0\\0 & 1\end{pmatrix}\in K,\ -U=\begin{pmatrix}-a & -b\\-(-b) & -a\end{pmatrix}\in K$$

şi acum este limpede că operaţiile induse satisfac axiomele inelului.

Fie $U\in K$, $U\neq 0$, $U=\begin{pmatrix}a & b\\-b & a\end{pmatrix}$. Cum $U\neq 0$, avem $a\neq 0$ sau $b\neq 0$, deci $a^2+b^2\neq 0$.

Fie

$$U'=\begin{pmatrix}\dfrac{a}{a^2+b^2} & \dfrac{-b}{a^2+b^2}\\[2ex] \dfrac{b}{a^2+b^2} & \dfrac{a}{a^2+b^2}\end{pmatrix}\in K.$$

O verificare imediată arată că

$$U'U=UU'=E,$$

deci U este inversabilă şi $U^{-1}=U'$. Aşadar, K este corp.

2) Fie $z\in\mathbb{C}$, $z=a+bi$ cu $a,b\in\mathbb{R}$. Definim

$$f(z)=\begin{pmatrix}a & b\\-b & a\end{pmatrix}\in K.$$

Dacă $z,w\in\mathbb{C}$, $z=a+bi$, $w=c+di$, atunci

$$z+w=(a+c)+(b+d)i,$$

$$zw=(ac-bd)+(ad+bc)i$$

deci

$$f(z+w)=\begin{pmatrix}a+c & b+d\\-(b+d) & a+c\end{pmatrix}=\begin{pmatrix}a & b\\-b & a\end{pmatrix}+\begin{pmatrix}c & d\\-a & c\end{pmatrix}=f(z)+f(w)$$

$$f(zw)=\begin{pmatrix}ac-bd & ad+bc\\-(ad+bc) & ac-bd\end{pmatrix}=\begin{pmatrix}a & b\\-b & a\end{pmatrix}\begin{pmatrix}c & d\\-d & c\end{pmatrix}=f(z)f(w).$$

Se mai observă că f este aplicaţie bijectivă, deci f este izomorfism, de unde $\mathbb{C}\simeq K$.

§ 6. POLINOAME CU COEFICIENŢI ÎNTR-UN INEL COMUTATIV

În clasa a X-a s-a dat o construcţie pentru polinoamele cu coeficienţi complecşi. Sub forma zisă *algebrică* un *polinom* f cu coeficienţi complecşi, într-o nedeterminată X, este o expresie de forma

$$f=a_0+a_1X+a_2X^2+\ldots+a_nX^n,$$

unde $a_i\in\mathbb{C}$ şi $n\geqslant 0$.

S-a notat cu $\mathbb{C}[X]$ mulţimea tuturor polinoamelor cu coeficienţi complecşi în nedeterminata X. Dacă $f,g\in\mathbb{C}[X]$, $f=a_0+a_1X+a_2X^2+\ldots$, $g=b_0+b_1X+b_2X^2+\ldots$ s-a definit *egalitatea*, *suma* şi *produsul* după cum urmează :

$$f=g\Leftrightarrow a_i=b_i,\ i=0,1,2,\ldots$$

$$f+g=(a_0+b_0)+(a_1+b_1)X+(a_2+b_2)X^2+\ldots$$

$$fg=a_0b_0+(a_0b_1+a_1b_0)X+(a_0b_2+a_1b_1+a_2b_0)X^2+\ldots$$

Din lista proprietăților adunării și înmulțirii polinoamelor cu coeficienți complecși, stabilite în clasa a X-a, rezultă :

$\mathbf{C}[X]$ *este inel comutativ în raport cu operațiile de adunare și înmulțire a polinoamelor.*

În construcția lui $\mathbf{C}[X]$, precum și în demonstrațiile proprietăților operațiilor cu polinoame, a intervenit, în mod esențial, faptul că adunarea și înmulțirea numerelor complexe satisfac axiomele inelului comutativ. Din acest motiv putem înlocui pe $\mathbf{C}$ cu un inel comutativ oarecare A. Se obține inelul comutativ $A[X]$ al polinoamelor cu coeficienți în A. Inelul A poate fi : inelul $\mathbf{Z}$ al întregilor raționali, inelul $\mathbf{Z}_n$ al claselor de resturi modulo n etc. În particular A poate fi un corp comutativ, de exemplu $\mathbf{Q}$, $\mathbf{R}$, $\mathbf{C}$, $\mathbf{Z}_p$, p număr prim. Obținem astfel inelele de polinoame

$$\mathbf{Z}[X],\ \mathbf{Z}_n[X],\ \mathbf{Q}[X],\ \mathbf{R}[X],\ \mathbf{C}[X],\ \mathbf{Z}_p[X]$$

cu coeficienți în $\mathbf{Z}$, $\mathbf{Z}_n$, $\mathbf{Q}$, $\mathbf{R}$, $\mathbf{C}$, $\mathbf{Z}_p$ respectiv.

Fie $f \in A[X]$, $f = a_0 + a_1X + \ldots + a_iX^i + \ldots$. Elementul $a_i \in A$ se numește *coeficientul* de rang i al polinomului f. Dacă $a_i = 0$, atunci termenul $0X^i$ poate fi omis, iar dacă $a_i = 1$, atunci termenul $1\,X^i$ poate fi scris simplu X^i. Dacă f este diferit de polinomul 0, atunci există $n \geqslant 0$ astfel încît $a_n \neq 0$ și $a_i = 0$, $\forall i > n$. În aceste condiții f va fi scris de regulă după cum urmează :

$$f = a_0 + a_1X + \ldots + a_nX^n.$$

Numărul $n = \max\,\{i | a_i \neq 0\}$ se numește *gradul* polinomului f, notat cu grad f, iar a_n se numește coeficientul *dominant* al lui f. Prin definiție, polinomul 0 are gradul $-\infty$.

Fie $f,\ g \in A[X]$ $\quad f = a_0 + a_1X + \ldots + a_nX^n,$

$$g = b_0 + b_1X + \ldots + b_mX^m$$

cu $a_n \neq 0$, $b_m \neq 0$. Pentru a face o alegere, presupunem că $n \geqslant m$. Atunci

$$f + g = (a_0 + b_0) + (a_1 + b_1)X + \ldots + (a_m + b_m)X^m + $$
$$+ a_{m+1}X^{m+1} + \ldots + a_nX^n$$

și

$$fg = a_0b_0 + (a_0b_1 + a_1b_0)X + \ldots + (\sum_{i+j=k} a_ib_j)X^k + \ldots + a_nb_mX^{m+n},$$

de unde

$$\text{grad}(f + g) \leqslant \max\,\{\text{grad } f,\ \text{grad } g\}$$

și

$$\text{grad }(fg) \leqslant \text{grad } f + \text{grad } g.$$

Formulele de mai sus rămîn adevărate și atunci cînd $f = 0$ sau $g = 0$. Dacă $n = m$ și $a_n = -b_n$, atunci în prima formulă avem inegalitatea strictă.

Dacă $f \neq 0$ și $g \neq 0$, iar A este inel fără divizori ai lui zero, atunci $fg \neq 0$ căci din $a_n \neq 0$ și $b_m \neq 0$ deducem că $a_nb_m \neq 0$. Mai mult, în acest caz

$$\text{grad }(fg) = \text{grad } f + \text{grad } g.$$

Așadar:

6.1. **Teoremă.** Dacă A este domeniu de integritate, atunci $A[X]$ este domeniu de integritate și

$$\text{grad}(fg) = \text{grad } f + \text{grad } g, \quad \forall f, g \in A[X].$$

Fie A un inel comutativ, $f \in A[X]$, $f = a_0 + a_1X + \ldots + a_nX^n$ și $x \in A$. Elementul $f(x) \in A$,

$$f(x) \overset{\text{def}}{=} a_0 + a_1x + \ldots + a_nx^n$$

se numește *valoarea* polinomului f în punctul x.

6.2. **Teoremă.** Valoarea sumei (produsului) a două polinoame $f, g \in A[X]$ într-un punct x este egală cu suma (respectiv produsul) valorilor polinoamelor f și g în punctul x:

$$(f + g)(x) = f(x) + g(x), \quad (fg)(x) = f(x)g(x).$$

Demonstrație. Dacă $f = a_0 + a_1X + a_2X^2 + \ldots$, $g = b_0 + b_1X + b_2X^2 + \ldots$, atunci pentru orice $x \in A$ avem:

$$f(x) + g(x) = (a_0 + a_1x + a_2x^2 + \ldots) + (b_0 + b_1x + b_2x^2 + \ldots) =$$
$$= (a_0 + b_0) + (a_1 + b_1)x + (a_2 + b_2)x^2 + \ldots = (f + g)(x)$$

și

$$f(x)g(x) = (a_0 + a_1x + a_2x^2 + \ldots)(b_0 + b_1x + b_2x^2 + \ldots) =$$
$$= a_0b_0 + (a_0b_1 + a_1b_0)x + (a_0b_2 + a_1b_1 + a_2b_0)x^2 + \ldots = (fg)(x).$$

Fie $f \in A[X]$. Asociind fiecărui element $x \in A$ valoarea $f(x)$ a polinomului f în punctul x se obține o funcție $\bar{f} : A \to A$,

$$\bar{f}(x) = f(x), \quad \forall x \in A,$$

numită *funcția polinomială* asociată lui f.

Zerourile funcției polinomiale $\bar{f} : A \to A$ asociată polinomului $f \in A[X]$ se numesc *rădăcini* (din A) ale lui f. Cu alte cuvinte, un element $a \in A$ se numește *rădăcină* (din A) a polinomului $f \in A[X]$ dacă valoarea lui f în punctul a este egală cu 0, deci $f(a) = 0$.

Exemple

1. Fie $f \in \mathbf{R}[X]$, $f = 7 - 6X + X^2$, atunci funcția polinomială asociată lui f este funcția reală de o variabilă reală $\bar{f} : \mathbf{R} \to \mathbf{R}$,

$$\bar{f}(x) = f(x) = 7 - 6x + x^2, \quad \forall x \in \mathbf{R}.$$

Rădăcinile (din $\mathbf{R}$) ale polinomului f sînt

$$x_{1,2} = 3 \pm \sqrt{3^2 - 7} = 3 \pm \sqrt{2}.$$

Funcțiile polinomiale asociate polinoamelor cu coeficienți reali sînt studiate în Analiză.

2. Dacă $f, g \in \mathbb{Z}_3[X]$, $f = X^3 + \hat{2}X^2 + X + \hat{1}$, $g = \hat{2}X^2 + \hat{2}X + \hat{1}$ (coeficienţii nespecificaţi sînt egali cu $\hat{1}$) atunci funcţiile polinomiale asociate $\bar{f} : \mathbb{Z}_3 \to \mathbb{Z}_3$, $\bar{g} : \mathbb{Z}_3 \to \mathbb{Z}_3$ pot fi descrise prin valorile lor în orice $x \in \mathbb{Z}_3$ folosind tabelele:

x	$\hat{0}$	$\hat{1}$	$\hat{2}$
$f(x)$	$\hat{1}$	$\hat{2}$	$\hat{1}$

x	$\hat{0}$	$\hat{1}$	$\hat{2}$
$g(x)$	$\hat{1}$	$\hat{2}$	$\hat{1}$

Se vede în acest caz că $f \neq g$ şi totuşi $\bar{f} = \bar{g}$.

Să mai observăm că polinoamele f şi g nu au rădăcini în $\mathbb{Z}_3$.

3. Polinomul $f = 2X - 7 \in \mathbb{Z}[X]$ nu are rădăcini în $\mathbb{Z}$. În adevăr, dacă pentru $a \in \mathbb{Z}$ avem $f(a) = 0$, atunci $2a - 7 = 0$, deci $2a = 7$. Dar $2a$ este par şi 7 este impar. Contradicţie.

4. Orice polinom f de grad 1 cu coeficienţi dintr-un corp comutativ K admite o rădăcină în K. În adevăr, fie $f \in K[X]$, $f = a + bX$, unde $a, b \in K$, $b \neq 0$. Fie $c = -b^{-1}a \in K$. Atunci

$$f(c) = a + bc = a + b(-b^{-1}a) = a - bb^{-1}a = a - a = 0.$$

5. Rădăcinile în $\mathbb{Z}_5$ ale polinomului $f \in \mathbb{Z}_5[X]$, $f = X^2 + \hat{1}$ sînt $\hat{2}$ şi $\hat{3}$. În adevăr, funcţia polinomială asociată, $\bar{f} : \mathbb{Z}_5 \to \mathbb{Z}_5$ ia valorile date în tabelul:

x	$\hat{0}$	$\hat{1}$	$\hat{2}$	$\hat{3}$	$\hat{4}$
$f(x)$	$\hat{1}$	$\hat{2}$	$\hat{0}$	$\hat{0}$	$\hat{2}$

Fie K un corp comutativ. Corpul K poate fi de exemplu $\mathbb{C}$, $\mathbb{R}$, $\mathbb{Q}$, $\mathbb{Z}_p$, p număr prim. Teorema de mai jos a fost demonstrată în clasa a X-a în cazul $K = \mathbb{C}$ şi demonstraţia s-a bazat în esenţă pe faptul că orice număr complex $z \neq 0$ are invers faţă de înmulţire. Din acest motiv rezultatul rămîne adevărat dacă în loc de $\mathbb{C}$ luăm un corp comutativ K oarecare. Aşadar:

6.3. Teoremă. **Fie K un corp comutativ şi $g \in K[X]$, $g \neq 0$. Oricare ar fi polinomul $f \in K[X]$, există polinoamele q, $r \in K[X]$ unic determinate astfel încît**

$$f = gq + r, \text{ grad } r < \text{grad } g.$$

Polinoamele q şi r se numesc *cîtul* respectiv *restul* împărţirii lui f prin g.

Exemplu

Fie $f, g \in \mathbb{Z}_5[X]$, $f = \hat{3}X^5 + \hat{4}X^4 + \hat{3}X^3 + \hat{3}X^2 + \hat{2}X + \hat{2}$, $g = \hat{2}X^2 + \hat{3}X + \hat{1}$. Să se afle cîtul şi restul împărţirii lui f prin g.

Coeficientul dominant al cîtului este elementul $a \in \mathbb{Z}_5$ care înmulţit cu coeficientul dominant al lui g dă coeficientul dominant al lui f. Deci $a \cdot \hat{2} = \hat{3}$, de unde $a = \hat{4}$.

Folosind tablele operaţiilor corpului $\mathbf{Z}_5$ şi organizarea uzuală a calculelor din algoritmul împărţirii polinoamelor, avem :

$$\begin{array}{rr|l}
& \hat{3}X^5 + \hat{4}X^4 + \hat{3}X^3 + \hat{3}X^2 + \hat{2}X + \hat{2} & \hat{2}X^2 + \hat{3}X + 1 \\
& \hat{3}X^5 + \hat{2}X^4 + \hat{4}X^3 \phantom{+ \hat{3}X^2 + \hat{2}X + \hat{2}} & \overline{\hat{4}X^3 + X^2 + \hat{3}X + \hat{4}} \\
\hline
/ & \hat{2}X^4 + \hat{4}X^3 + \hat{3}X^2 + \hat{2}X + \hat{2} & \\
& \hat{2}X^4 + \hat{3}X^3 + X^2 \phantom{+ \hat{2}X + \hat{2}} & \\
\hline
& X^3 + \hat{2}X^2 + \hat{2}X + \hat{2} & \\
& X^3 + \hat{4}X^2 + \hat{3}X \phantom{+ \hat{2}} & \\
\hline
/ & \hat{3}X^2 + \hat{4}X + \hat{2} & \\
& \hat{3}X^2 + \hat{2}X + \hat{4} & \\
\hline
/ & \hat{2}X + \hat{3} &
\end{array}$$

Rezultă că $q = \hat{4}X^3 + X^2 + \hat{3}X + \hat{4}$ şi $r = \hat{2}X + \hat{3}$. Avem :

$$gq + r = (\hat{2}X^2 + \hat{3}X + \hat{1})\,(\hat{4}X^3 + X^2 + \hat{3}X + \hat{4}) + \hat{2}X + \hat{3} =$$
$$= \hat{3}X^5 + \hat{4}X^4 + \hat{3}X^3 + \hat{3}X^2 + \hat{2}X + \hat{2} = f.$$

Fie $f, g \in K[X]$. Vom spune că polinomul g *divide* polinomul f şi scriem $g|f$, dacă există $q \in K[X]$ astfel încît $f = gq$. Se mai spune în acest caz că g este *divizor* sau *factor* al lui f în inelul $K[X]$ sau că f este *multiplu* al lui g în inelul $K[X]$.

Calculul valorii $f(a)$ a unui polinom $f \in K[X]$ într-un punct $a \in K$ poate fi făcut cu algoritmul împărţirii polinoamelor. În adevăr:

6.4. Teorema restului. **Fie K un corp comutativ, $f \in K[X]$ şi $a \in K$. Atunci valoarea $f(a)$ a polinomului f în punctul a este egală cu restul împărţirii lui f prin $X - a$.**

Demonstraţie. Fie $q, r \in K[X]$ astfel încît

$$f(x) = (X - a)q + r, \text{ grad } r < \text{grad } (X - a) = 1.$$

Rezultă că $r \in K$ şi deci

$$f(a) = ((X - a)q + r)\,(a) = (a - a)q(a) + r(a) = r(a) = r.$$

Tot ca o consecinţă a Teoremei 6.3 putem obţine o caracterizare a divizorilor de grad 1 ai unui polinom, anume :

6.5. Teorema factorului. (Bézout). Fie K un corp comutativ, $f \in K[X]$ şi $a \in K$. Atunci polinomul $X - a$ divide pe f dacă şi numai dacă $f(a) = 0$.

Demonstrație. Evident $X - a$ divide f dacă și numai dacă restul r al împărțirii este 0. Afirmația rezultă din faptul că $r = f(a)$.

Împărțirea unui polinom $f \in K[X]$ prin $X - a$ (deci și calculul valorii $f(a)$) se poate face cu schema lui Horner.

Exerciții rezolvate

R — 1 Să se determine două polinoame $f, g \in \mathbb{Z}[X]$ astfel încît $fg = -1 + 6X - 12X^2 + 8X^3$, grad $f = 1$ și grad $g = 2$.

Soluție. Conform condițiilor din enunț avem $f = a_0 + a_1X$, $g = b_0 + b_1X + b_2X^2$, unde $a_i, b_j \in \mathbb{Z}$, $a_1 \neq 0$ și $b_2 \neq 0$. Avem:

$$fg = a_0b_0 + (a_0b_1 + a_1b_0)X + (a_0b_2 + a_1b_1)X^2 + a_1b_2X^3 = -1 + 6X - 12X^2 + 8X^3,$$

de unde, conform definiției egalității polinoamelor, deducem:

$$\begin{cases} a_0b_0 = -1, \\ a_0b_1 + a_1b_0 = 6, \\ a_0b_2 + a_1b_1 = -12 \\ a_1b_2 = 8. \end{cases}$$

Dar, din $a_0b_0 = -1$ cu $a_0, b_0 \in \mathbb{Z}$ rezultă $a_0 = 1$, $b_0 = -1$ sau $a_0 = -1$, $b_0 = 1$. Cînd $a_0 = 1$, $b_0 = -1$, avem:

$$\begin{cases} b_1 - a_1 = 6, \\ b_2 + a_1b_1 = -12, \\ a_1b_2 = 8, \end{cases}$$

de unde $a_1 = -2$, $b_1 = 4$, $b_2 = -4$, deci $f = 1 - 2X$ și $g = -1 + 4X - 4X^2$. Cînd $a_0 = -1$, $b_0 = 1$ se găsește $f = -1 + 2X$ și $g = 1 - 4X + 4X^2$.

R — 2 Determinați toate polinoamele $f \in \mathbb{Z}_4[X]$ astfel încît

$$f^2 = \hat{0} \text{ și grad } f = 1.$$

Aceeași problemă pentru polinoamele inelului $\mathbb{Z}_5[X]$.

Soluție. Fie $f = \hat{a} + \hat{b}X \in \mathbb{Z}_4[X]$, $\hat{b} \neq \hat{0}$. Cum $f^2 = \hat{0}$ rezultă că

$$0 = f^2 = (\hat{a} + \hat{b}X)(\hat{a} + \hat{b}X) = \hat{a}^2 + 2\hat{a}\hat{b}X + \hat{b}^2X^2$$

și deci, prin identificarea coeficienților, avem:

$$(S) \begin{cases} \hat{a}^2 = \hat{0}, \\ 2\hat{a}\hat{b} = \hat{0}, \\ \hat{b}^2 = \hat{0}. \end{cases}$$

Dar $\mathbb{Z}_4 = \{\hat{0}, \hat{1}, \hat{2}, \hat{3}\}$ și $\hat{0}^2 = \hat{0}$, $\hat{1}^2 = \hat{1}$, $\hat{2}^2 = \hat{0}$, $\hat{3}^2 = \hat{1}$.

Rezultă că soluţiile sistemului (S) sînt $(\hat{0}, \hat{0})$, $(\hat{0}, \hat{2})$, $(\hat{2}, \hat{0})$ şi $(\hat{2}, \hat{2})$. Cum $\hat{b} \neq \hat{0}$, deducem că polinoamele căutate sînt $\hat{2}X$ şi $\hat{2} + \hat{2}X$.

Observăm că $\mathbf{Z}_5$ este corp, deci inelul $\mathbf{Z}_5[X]$ nu are divizori ai lui zero şi atunci din $f^2 = \hat{0}$ rezultă $f = \hat{0}$.

R — 3 Fie $f \in \mathbf{Z}_5[X]$, $f = X^3 + \hat{3}X + \hat{4}$. Să se afle cîtul şi restul împărţirii lui f prin polinomul $X + \hat{3}$.

Soluţie. Avem $\hat{3} = -\hat{2}$ deoarece $-\hat{2} = \widehat{-2} = \widehat{0 - 2} = \widehat{5 - 2} = \hat{3}$, deci $X + \hat{3} = X - \hat{2}$ şi folosind schema lui Horner

$\hat{1}$	$\hat{0}$	$\hat{3}$	$\hat{4}$	
$\hat{1}$	$\hat{2}$	$\hat{2}$	$\hat{3}$	$\hat{2}$

deducem că $q = X^2 + \hat{2}X + \hat{2}$ şi $r = \hat{3} = f(\hat{2})$.

R — 4 Fie $f \in \mathbf{Z}_2[X]$, $f = a_0 + a_1X + \ldots + a_nX^n$. Arătaţi că f se divide prin $X + \hat{1}$ dacă şi numai dacă f are un număr par de coeficienţi $a_i \neq \hat{0}$.

Soluţie. Cum $\hat{1} + \hat{1} = \hat{0}$, avem $X + \hat{1} = X - \hat{1}$. Dar

$$f(\hat{1}) = a_0 + a_1 + \ldots + a_n$$

şi cum $\hat{1} + \hat{1} = \hat{0}$, rezultă că $f(\hat{1}) = \hat{0}$ dacă şi numai dacă numărul coeficienţilor $a_i \neq \hat{0}$ este par. Se aplică apoi teorema factorului.

R — 5 Fie K un corp comutativ, $f \in K[X]$ şi $a, b \in K$, $a \neq b$.

1) Arătaţi că restul împărţirii polinomului f prin $(X - a)(X - b)$ este

$$\frac{f(a) - f(b)}{a - b} X + \frac{af(b) - bf(a)}{a - b}.$$

2) Dacă $X - a \mid f$, $X - b \mid f$ şi $a \neq b$, atunci $(X - a)(X - b) \mid f$.

Soluţie. 1) Cum gradul polinomului $(X - a)(X - b)$ este egal cu 2, restul împărţirii lui f prin g este de forma $cX + d$, cu $c, d \in K$. Fie $q \in K[X]$ astfel încît

$$f = (X - a)(X - b)q + cX + d.$$

Deducem că $f(a) = ca + d$ şi $f(b) = cb + d$ şi cum $a \neq b$ avem: $c = (a - b)^{-1}(f(a) - f(b))$ şi $d = (a - b)^{-1}(af(b) - bf(a))$.

2) Dacă $X - a \mid f$ şi $X - b \mid f$, atunci $f(a) = f(b) = 0$. Se deduce că $c = d = 0$, deci $f = (X - a)(X - b)q$

§ 7. POLINOAME IREDUCTIBILE. DESCOMPUNEREA POLINOAMELOR ÎN PRODUS DE FACTORI IREDUCTIBILI

Fie K un corp comutativ și $K[X]$ inelul polinoamelor în nedeterminata X cu coeficienți în K. Vom arăta că aritmetica inelului $K[X]$ este în esență aceeași cu cea a inelului $\mathbf{Z}$ al întregilor raționali. Se știe că pentru orice număr întreg $a > 1$ există numerele prime $p_i > 0$, $1 \leqslant i \leqslant n$, unic determinate astfel încît $a = p_1 p_2, \ldots, p_n$, rezultat cunoscut sub numele de *teorema fundamentală a aritmeticii*. Un rezultat asemănător este adevărat și pentru polinoamele cu coeficienți într-un corp comutativ K, locul numerelor prime fiind luat de către polinoamele ireductibile (v. Teorema 7.2)

7.1. *Definiție.* Fie K un corp comutativ și $f \in K[X]$ un polinom de grad $n > 0$. Spunem că f este polinom *reductibil* peste corpul K dacă există două polinoame $g, h \in K[X]$ de grad strict mai mic ca n astfel încît $f = gh$. În caz contrar, spunem că f este polinom *ireductibil* peste corpul K.

Exemple

1. *Orice polinom de grad* 1 din $K[X]$ *este ireductibil peste* K. În adevăr, fie $f = aX + b$, $a \neq 0$, un polinom de grad 1 din $K[X]$. Dacă f este reductibil peste K există $g, h \in K[X]$, astfel încît

$$f = gh, \text{ grad } g < 1, \text{ grad } h < 1.$$

Evident $g \neq 0$ și $h \neq 0$, de unde grad $g =$ grad $h = 0$.
Obținem $1 = \text{grad } f = \text{grad } (gh) = \text{grad } g + \text{grad } h = 0 + 0 = 0$.
Contradicție. Deci f este ireductibil peste K.

2. *Dacă un polinom* $f \in K[X]$ de grad $n > 1$ *este ireductibil peste* K, *atunci* f *nu admite rădăcini în* K. *Reciproc, dacă un polinom* $f \in K[X]$ *de grad* 2 *sau* 3 *nu admite rădăcini în* K, *atunci* f *este ireductibil peste* K.

În adevăr, dacă grad $f = n > 1$ și $a \in K$ este rădăcină a lui f, atunci conform teoremei factorului $X - a \mid f$, deci există $q \in K[X]$ astfel încît

$$f = (X - a)q.$$

Cum $X - a, q \in K[X]$ și grad $(X - a) = 1 < n$, grad $q = n - 1 < n$ rezultă că f este reductibil peste K.

Reciproc, presupunem că gradul lui f este 2 sau 3. Dacă f este reductibil peste K, atunci f admite o rădăcină în K. În adevăr, fie $g, h \in K[X]$ astfel încît

$$f = gh, \text{ grad } g < \text{grad } f, \text{ grad } h < \text{grad } f.$$

Cum grad f = grad g + grad h, iar grad f este 2 sau 3, rezultă grad $g = 1$ sau grad $h = 1$. Presupunem că grad $g = 1$. Atunci $g = aX + b \in K[X]$, $a \neq 0$. Fie $c = -a^{-1}b \in K$. Avem

$$f(c) = g(c)h(c) = (a(-a^{-1}b) + b)h(c)) = 0 \cdot h(c) = 0.$$

Astfel, polinomul $f = X^2 - 2 \in \mathbf{Q}[X]$ este ireductibil peste $\mathbf{Q}$. În adevăr, în caz contrar există $a \in \mathbf{Q}$ astfel încît $0 = f(a) = a^2 - 2$, de unde $\sqrt{2} = a \in \mathbf{Q}$. Contradicție.

Să observăm că același polinom $f = X^2 - 2$ este reductibil peste $\mathbf{R}$ căci $f = (X - \sqrt{2})(X + \sqrt{2})$ și $X - \sqrt{2}$, $X + \sqrt{2} \in \mathbf{R}[X]$.

Polinomul $f = X^3 + \hat{2}X^2 + X + \hat{1} \in \mathbf{Z}_3[X]$ este ireductibil peste corpul $\mathbf{Z}_3$. În adevăr, grad $f = 3$ și $f(\hat{0}) = \hat{1} \neq \hat{0}$, $f(\hat{1}) = \hat{2} \neq \hat{0}$, $f(\hat{2}) = \hat{1} \neq \hat{0}$.

3. *Polinoamele de grad* 1 *din* $\mathbf{C}[X]$ *sînt singurele polinoame ireductibile peste corpul* $\mathbf{C}$. În adevăr, din Exp. 1 rezultă că polinoamele de grad 1 din $\mathbf{C}[X]$ sînt ireductibile peste $\mathbf{C}$. Fie acum $f \in \mathbf{C}[X]$, astfel încît grad $f > 1$.

Să arătăm că f este reductibil peste $\mathbf{C}$. Conform teoremei fundamentale a algebrei (d' Alembert-Gauss) există $z \in \mathbf{C}$ astfel încît $f(z) = 0$. Din Exp. 2 rezultă că f este reductibil peste $\mathbf{C}$.

4. *Polinoamele de grad* 1 *și polinoamele de grad* 2 *fără rădăcini reale din* $\mathbf{R}[X]$ *sînt singurele polinoame ireductibile peste corpul* $\mathbf{R}$. Este suficient să arătăm că orice polinom $f \in \mathbf{R}[X]$ ireductibil peste $\mathbf{R}$ și de grad $n > 1$ este polinom de grad 2 fără rădăcini reale (v. Exp. 1 și 2). Conform teoremei fundamentale a algebrei există $z = a + ib \in \mathbf{C}$ astfel încît $f(z) = 0$. Avem $b \neq 0$ căci în caz contrar $z = a \in \mathbf{R}$ și atunci f ar fi reductibil peste $\mathbf{R}$ (v. Exp. 2).

Cum polinomul f are coeficienți reali, avem și $f(\bar{z}) = 0$, unde $\bar{z} = a - ib$. Deoarece $\mathbf{R}[X] \subset \mathbf{C}[X]$, avem $f \in \mathbf{C}[X]$, $f(z) = 0$, $f(\bar{z}) = 0$, deci în inelul $\mathbf{C}[X]$ polinomul f se divide prin $X - z$ și $X - \bar{z}$. Dar $b \neq 0$, deci $z \neq \bar{z}$ și atunci (v. Ex. R—5, § 6) deducem că polinomul:

$$(X - z)(X - \bar{z}) = X^2 - 2aX + a^2 + b^2 \in \mathbf{R}[X]$$

divide pe f. Deducem că există $q \in \mathbf{R}[X]$ astfel încît

$$(*) \qquad f = (X^2 - 2aX + a^2 + b^2)q.$$

Dacă $n > 2$, atunci din (*) rezultă că f este reductibil peste $\mathbf{R}$, contrar ipotezei. Așadar, $n = 2$, $q \in \mathbf{R}$, $q \neq 0$, de unde rezultă că f este un polinom de grad 2 fără rădăcini reale.

Fie $f, g \in K[X]$. Spunem că f este *asociat în divizibilitate* cu g și scriem $f \sim g$, dacă există $a \in K$, $a \neq 0$, astfel încît $f = ag$.

Putem acum enunța următorul rezultat care generalizează la polinoame cu coeficienți într-un corp comutativ teorema fundamentală a aritmeticii :

7.2. Teoremă. Fie K un corp comutativ și $f \in K[X]$ un polinom de grad mai mare ca 0. Atunci :

1) f se descompune într-un produs finit de polinoame ireductibile peste K.

2) Dacă $f = f_1 f_2 \dots f_m = f'_1 f'_2 \dots f'_{m'}$ sînt două descompuneri ale polinomului f în produs finit de polinoame ireductibile, atunci $m = m'$ și există o permutare $\sigma \in \mathfrak{S}_m$ astfel încît $f_i \sim f'_{\sigma(i)}$, $1 \leqslant i \leqslant m$.

Demonstrație. Vom demonstra numai afirmația 1). Fie $n = \text{grad } f$. Dacă $n = 1$, atunci f este ireductibil peste K și deci 1) este adevărat (printre produsele finite acceptăm și produsele cu un singur factor).

Presupunem că $n > 1$ și că afirmația 1) este adevărată pentru polinoame de grad mai mic ca n. Dacă f este ireductibil atunci 1) este adevărat. În caz contrar există $g, h \in K[X]$ astfel încît $f = gh$, grad $g < n$, grad $h < n$. Conform ipotezei inducției g și h sînt produse finite de polinoame ireductibile peste K, deci și $f = gh$ este un produs finit de polinoame ireductibile peste K.

7.3. *Consecință.* **Orice polinom $f \in \mathbb{C}[X]$ de grad mai mare ca 0 se reprezintă ca produs finit de polinoame de grad 1 din $\mathbb{C}[X]$, unic determinate mai puțin ordinea și o asociere în divizibilitate a factorilor.**

Demonstrație. Rezultă din Teorema 7.2 și Exp. 4.

7.4. *Consecință.* **Orice polinom $f \in \mathbb{R}[X]$ de grad mai mare ca 0 se reprezintă ca produs finit de polinoame din $\mathbb{R}[X]$ de grad 1 sau de grad 2 fără rădăcini reale, unic determinate mai puțin ordinea și o asociere în divizibilitate a factorilor.**

Demonstrație. Rezultă din Teorema 7.2 și Exp. 4.

Exerciții rezolvate

R—1 Să se descompună în factori ireductibili peste $\mathbb{Q}$, $\mathbb{R}$ și $\mathbb{C}$ polinomul $f = X^4 + X^3 - X^2 - 2X - 2$ știind că admite rădăcina $z = -\frac{1}{2} + i\frac{\sqrt{3}}{2}$.

Soluție. Polinomul f avînd coeficienții reali, admite și rădăcina $\bar{z} = -\frac{1}{2} - i\frac{\sqrt{3}}{2}$, deci f se divide prin polinomul $(X - z)(X - \bar{z}) = X^2 + X + 1$ (v. Ex. R—5, § 6). Obținem:

$$f = (X^2 - 2)(X^2 + X + 1). \tag{1}$$

Cum rădăcinile polinomului $X^2 + X + 1$ sînt complexe rezultă că $X^2 + X + 1$ este ireductibil peste $\mathbb{R}$ și cu atît mai mult peste $\mathbb{Q}$. Am observat că $X^2 - 2$ este ireductibil peste $\mathbb{Q}$ (v. Exp. 2). Așadar, (1) este descompunerea lui f în factori ireductibili peste $\mathbb{Q}$. Descompunerile lui f în factori ireductibili peste $\mathbb{R}$ și $\mathbb{C}$ sînt:

$$f = (X - \sqrt{2})(X + \sqrt{2})(X^2 + X + 1).$$

respectiv

$$f = (X - \sqrt{2})(X + \sqrt{2})\left(X + \frac{1}{2} - i\frac{\sqrt{3}}{2}\right)\left(X + \frac{1}{2} + i\frac{\sqrt{3}}{2}\right).$$

R—2 Să se descompună în factori ireductibili peste corpul $\mathbf{Z}_3$ polinomul $f = X^3 + \hat{2}X^2 + X + \hat{2} \in \mathbf{Z}_3[X]$.

Soluție. Pentru a valorifica observațiile făcute la Exp. 2, să cercetăm valorile $f(x)$, $x \in \mathbf{Z}_3$. Avem :

x	$\hat{0}$	$\hat{1}$	$\hat{2}$
$f(x)$	$\hat{2}$	$\hat{0}$	$\hat{2}$

deci f se divide prin $X - \hat{1} = X + \hat{2}$. Folosind schema lui Horner

$\hat{1}$	$\hat{2}$	$\hat{1}$	$\hat{2}$	
$\hat{1}$	$\hat{0}$	$\hat{1}$	$\hat{0}$	$\hat{1}$

obținem $f = (X - \hat{1})(X^2 + \hat{1})$. Cum $X^2 + 1$ nu are rădăcini în $\mathbf{Z}_3$ rezultă că este ireductibil peste $\mathbf{Z}_3$. Descompunerea căutată este $f = (X - \hat{1})(X^2 + \hat{1}) = (X + \hat{2})(X^2 + \hat{1})$.

R—3 1) Cîte polinoame de grad cel mult 4 sînt în inelul $\mathbf{Z}_2[X]$?

2) Să se găsească toate polinoamele de grad cel mult 4 ireductibile peste corpul $\mathbf{Z}_2$.

Soluție. 1) Dacă $f \in \mathbf{Z}_2[X]$ are gradul cel mult 4, atunci

$$f = a_0 + a_1X + a_2X^2 + a_3X^3 + a_4X^4 \ (a_i \in \mathbf{Z}_2).$$

Cum pentru fiecare coeficient a_i avem două posibilități, $\hat{0}$ sau $\hat{1}$, din definiția egalității polinoamelor rezultă că avem $2^5 = 32$ polinoame de grad cel mult 4.

2) Singurele polinoame de grad 1 sînt X, $\hat{1} + X$ și acestea sînt ireductibile peste $\mathbf{Z}_2$ (v. Exp. 1).

Un polinom ireductibil peste $\mathbf{Z}_2$ de grad 2, 3 sau 4 are termenul liber egal cu $\hat{1}$ căci altfel admite ca rădăcină pe $\hat{0} \in \mathbf{Z}_2$ și deci ar fi reductibil peste $\mathbf{Z}_2$. De asemenea, numărul coeficienților $\neq \hat{0}$ ai unui asemenea polinom este impar căci altfel ar admite pe $\hat{1} \in \mathbf{Z}_2$ ca rădăcină (v. Ex. R—4, § 6) și deci ar fi reductibil peste $\mathbf{Z}_2$. Singurele polinoame de grad 2 sau 3 care satisfac ambele condiții sînt $\hat{1} + X + X^2$, $\hat{1} + X + X^3$, $\hat{1} + X^2 + X^3$ și conform cu observațiile de la Exp. 2 ele sînt ireductibile peste $\mathbf{Z}_2$.

În fine, singurele polinoame de grad 4 care satisfac cele două condiții sînt $\hat{1} + X + X^4$, $\hat{1} + X^2 + X^4$, $\hat{1} + X^3 + X^4$, $\hat{1} + X + X^2 + X^3 + X^4$ și fie f unul dintre ele. Dacă f este reductibil, descompunerea sa în factori ireductibili nu poate conține factori de gradul 1 căci atunci $f(\hat{0}) = \hat{0}$ sau $f(\hat{1}) = \hat{0}$, ceea ce am exclus.

Acum este clar că descompunerea lui f nu poate conține nici factori ireductibili de grad 3 (căci atunci ar conține și unul de grad 1). Atunci descompunerea lui f conține numai factori ireductibili de grad 2. Cum $\hat{1} + X + X^2$ este singurul polinom ireductibil de grad 2, iar grad $f = 4$, rezultă că

$$f = (\hat{1} + X + X^2)^2 = \hat{1} + X^2 + X^4.$$

Aşadar, polinoamele ireductibile de grad 4 sînt $\hat{1} + X + X^4$, $\hat{1} + X^3 + X^4$ şi $1 + X + X^2 + X^3 + X^4$.

Remarcă. Polinoamele ireductibile peste corpul Z_2 au aplicaţii în teoria codurilor (v. § 8, pct. 2).

§ 8. APLICAŢII ALE CORPURILOR FINITE (facultativ)

1. PĂTRATE LATINE

Să presupunem că într-o anumită zonă agricolă trebuie să comparăm productivitatea a patru hibrizi de porumb : A, B, C şi D. Pentru testarea acestora dispunem de un teren în formă de pătrat. Se pune problema să organizăm de aşa natură experimentul încît să reducem erorile care pot fi introduse de variaţiile de fertilitate a terenului. Putem compensa erorile care apar datorită variaţiilor de fertilitate împărţind terenul în 16 parcele egale (v. fig. IV.1, *a*) şi cultivînd apoi în fiecare parcelă cîte unul din hibrizii de porumb astfel încît în fiecare linie şi în fiecare coloană de parcele, fiecare hibrid de porumb să fie cultivat o dată si numai o singură dată.

?	?	?	?
?	?	?	?
?	?	?	?
?	?	?	?

a

+	0	1	*a*	*b*
0	0	1	*a*	*b*
1	1	0	*b*	*a*
a	*a*	*b*	0	1
b	*b*	*a*	1	0

b

A	*B*	*C*	*D*
B	*A*	*D*	*C*
C	*D*	*A*	*B*
D	*C*	*B*	*A*

c

Fig. IV.1.

Este posibilă o asemenea organizare a experimentului ? Să ne amintim că în tabla operaţiei unui grup orice element al grupului apare, pe fiecare linie şi fiecare coloană, o dată şi numai o singură dată (v. Ex. **R**—2, Cap. III, § 3). Acum răspunsul la întrebarea pusă este evident. Considerăm tabla operaţiei unui grup cu patru elemente, de exemplu tabla adunării grupului aditiv al corpului de la Ex. **R**—**1**, § 4, pe care am reprodus-o în fig. IV.1, *b*. Pe poziţiile ocupate în tablă de elementele 0, 1, *a* şi *b* punem A, B, C şi D respectiv şi obţinem organizarea dorită pentru experimentul nostru (v. fig. IV.1, c).

Să ridicăm acum gradul de dificultate a problemei noastre. Anume, să presupunem că avem şi patru tipuri de erbicide, α, β, γ şi δ, pe care vrem să le folosim pe cele 16 parcele astfel încît fiecare hibrid de porumb să fie cuplat o dată şi numai o singură dată cu fiecare tip de erbicid.

α	β	γ	δ
γ	δ	α	β
δ	γ	β	α
β	α	δ	γ

a

$A\alpha$	$B\beta$	$C\gamma$	$D\delta$
$B\gamma$	$A\delta$	$D\alpha$	$C\beta$
$C\delta$	$D\gamma$	$A\beta$	$B\alpha$
$D\beta$	$C\alpha$	$B\delta$	$A\gamma$

b

Fig. IV.2.

Dacă erbicidele sînt folosite pe cele 16 parcele ca în figura IV.2, *a*, atunci cerința pusă este satisfăcută (v. fig. IV.2, *b*). Rămîne să explicăm cum am stabilit modul de folosire a erbicidelor ca să fie satisfăcută condiția pusă.

Să dăm mai întîi două definiții.

Fie M o mulțime cu n elemente. Un tablou L cu n linii și n coloane de elemente din M se numește *pătrat latin* de ordin n peste mulțimea M dacă fiecare element al lui M apare o dată și numai o dată în fiecare linie și în fiecare coloană.

Astfel, tabloul de la figura IV.1, *c* este pătrat latin de ordin 4 peste mulțimea $M = \{A, B, C, D\}$, iar tabloul de la figura IV.2, *a* este pătrat latin de ordin 4 peste mulțimea $N = \{\alpha, \beta, \gamma, \delta\}$. Tabla operației unui grup G cu n elemente este un pătrat latin de ordin n peste G.

Evident, pentru a forma un pătrat latin de ordin n peste o mulțime M cu n elemente avem nevoie de n „copii" ale fiecărui element din M.

Două pătrate latine de ordin n se numesc *ortogonale* dacă prin suprapunere fiecare element al primului pătrat latin se cuplează o dată și numai o singură dată cu fiecare element al celui de al doilea pătrat latin.

Pătratul latin de la figura IV.1, *c* este ortogonal cu cel de la figura IV.2, *a*, altfel spus, prin suprapunere obținem elementele produsului cartezian $M \times N$ (v. fig. IV.2, *b*).

Dacă avem un corp cu n elemente, atunci sîntem asigurați că există $n - 1$ pătrate latine ortogonale două cîte două. Mai precis :

Teoremă. Fie $K = \{x_0, x_1, \ldots, x_{n-1}\}$ un corp cu n elemente, unde elementul 0 s-a notat cu x_0 și elementul 1 s-a notat cu x_1. Fie $u \in K \setminus \{0\}$. Notăm cu L_u tabloul cu n linii și n coloane care la intersecția liniei i cu coloana j conține elementul

$$x_{ij}^u \overset{\text{def}}{=} ux_i + x_j,\ 0 \leqslant i,\ j < n.$$

1) L_u este pătrat latin de ordin n peste K.

2) Dacă $u, v \in K \setminus \{0\}$, $u \neq v$, atunci L_u și L_v sînt pătrate latine ortogonale.

Demonstrație

1) Fie x_{ij}^u și x_{it}^u două elemente de linia i a lui L_u, unde $j \neq t$. Dacă $x_{ij}^u = x_{it}^u$, atunci $ux_i + x_j = ux_i + x_t$. Rezultă că $x_j = x_t$, deci $j = t$. Contradicție. Rămîne adevărat că pe linia i a lui L_u avem n elemente distincte din K. Cum $|K| = n$ deducem că fiecare element al lui K apare o dată și numai o singură dată pe linia i, $0 \leqslant i < n$*.

Fie acum x_{ij}^u și x_{sj}^u două elemente de pe coloana j a lui L_u, unde $i \neq s$. Dacă $x_{ij}^u = x_{sj}^u$, atunci $ux_i + x_j = ux_s + x_j$. Rezultă $ux_i = ux_s$ și cum $u \neq 0$, avem $x_i = x_s$, deci $i = s$. Contradicție. Se deduce că pe coloana j a lui L_u fiecare element al lui K apare o dată și numai o singură dată.

2) Presupunem că L_u și L_v nu sînt ortogonale. Atunci există două poziții distincte (i, j) și (s, t) unde după suprapunerea lui L_u și L_v obținem același cuplu de elemente din K, adică $(x_{ij}^u, x_{ij}^v) = (x_{st}^u, x_{st}^v)$. Așadar $x_{ij}^u = x_{st}^u$ și $x_{ij}^v = x_{st}^v$, adică $ux_i + x_j = ux_s + x_t$ și $vx_i + x_j = vx_s + x_t$. Scăzînd termen cu termen ultimele două egalități, obținem $(u - v)(x_i - x_s) = 0$. Cum $u \neq v$ și K este corp, deducem $x_i = x_s$, deci $i = s$. Acum din $ux_i + x_j = ux_s + x_t$ și $i = s$, deducem că avem și $j = t$, deci $(i, j) = (s, t)$. Contradicție.

Să considerăm din nou tablele operațiilor corpului K cu patru elemente de la Ex. R−1, § 4.

+	0	1	*a*	*b*
0	0	1	*a*	*b*
1	1	0	*b*	*a*
a	*a*	*b*	0	1
b	*b*	*a*	1	0

·	0	1	*a*	*b*
0	0	0	0	0
1	0	1	*a*	*b*
a	0	*a*	*b*	1
b	0	*b*	1	*a*

* Se notează cu $|M|$ numărul elementelor mulțimii M.

Cum K are trei elemente diferite de 0, anume 1, a și b, cu construcția de la teorema precedentă obținem trei pătrate latine L_1, L_a și L_b de ordin 4 peste K, ortogonale două cîte două, anume:

$$L_1 = \begin{bmatrix} 0 & 1 & a & b \\ 1 & 0 & b & a \\ a & b & 0 & 1 \\ b & a & 1 & 0 \end{bmatrix}, \quad L_a = \begin{bmatrix} 0 & 1 & a & b \\ a & b & 0 & 1 \\ b & a & 1 & a \\ 1 & 0 & b & a \end{bmatrix}, \quad L_b = \begin{bmatrix} 0 & 1 & a & b \\ b & a & 1 & 0 \\ 1 & 0 & b & a \\ a & b & 0 & 1 \end{bmatrix}$$

Cum $x^1_{ij} = 1 \cdot x_i + x_j = x_i + x_j$, rezultă că L_1 provine direct din tabla adunării corpului K. Și pătratele latine L_a și L_b pot fi completate folosind tabelele operațiilor corpului K. Astfel, pentru a completa linia a 3-a a lui L_a să observăm că $x^a_{2j} = ax_2 + xj = a \cdot a + xj$. Din tabla înmulțirii lui K rezultă că $a \cdot a = b$, deci $x_{2j} = b + x_j$, $0 \leqslant j < 4$. Așadar, linia a 3-a a lui L_a coincide cu linia lui b din tabla adunării lui K.

Să observăm acum că înlocuind în L_a elementele 0, 1, a și b cu α, β, γ și δ respectiv, se obține pătratul latin de la figura IV.2, a care este ortogonal cu cel de la figura IV.1, c, care la rîndul său se obține din L_1 înlocuind pe 0, 1, a și b cu A, B, C și D respectiv.

Într-o problemă datînd din 1779 L. Euler a conjecturat că este imposibil să fie aranjați la o paradă 36 de ofițeri de șase grade diferite și provenind din șase regimente într-un careu cu 6 linii și 6 coloane, astfel încît în fiecare linie și în fiecare coloană să fie reprezentat fiecare grad și fiecare regiment. Evident, aceasta revine la a găsi două pătrate latine de ordin 6 ortogonale. Abia în 1899 s-a demonstrat că nu există două pătrate latine de ordin 6 ortogonale.

2. CODIFICAREA MESAJELOR

Fie A o mulțime cu două elemente, anume simbolurile 0 și 1. Mulțimea A va fi numită *alfabet*, iar simbolurile 0 și 1 sînt numite *literele* alfabetului A. Cu ajutorul literelor alfabetului A putem forma 2^n secvențe diferite cu cîte n termeni,

$$a_0a_1 \ldots a_{n-1}, \quad (a_i \in A)$$

numite *cuvinte* de lungime n peste alfabetul A. Notăm cu D_n mulțimea tuturor cuvintelor de lungime n peste alfabetul A. Dacă $x, y \in D_n$, $x = a_0a_1, \ldots, a_{n-1}$, $y = b_0b_1, \ldots, b_{n-1}$, atunci numărul de indici i pentru care $a_i \neq b_i$ se numește *distanța Hamming* dintre cuvintele x și y și va fi notată cu $\mathrm{d}(x, y)$. Se verifică ușor că

$$\mathrm{d}(x, y) \leqslant \mathrm{d}(x, z) + \mathrm{d}(z, y), \ \forall\, x, y, z \in D_n.$$

Avem $2^3 = 8$ cuvinte de lungime 3 peste alfabetul $A = \{0, 1\}$, anume

$$D_3 = \{000, 100, 010, 001, 110, 011, 101, 111\}.$$

Dacă $x = 110$ și $y = 101$, atunci $\mathrm{d}(x, y) = 2$. Cuvintele din D_3 pot fi puse în corespondență biunivocă cu vîrfurile unui cub ca în figura IV.3, distanța Hamming dintre două vîrfuri vecine fiind egală cu 1.

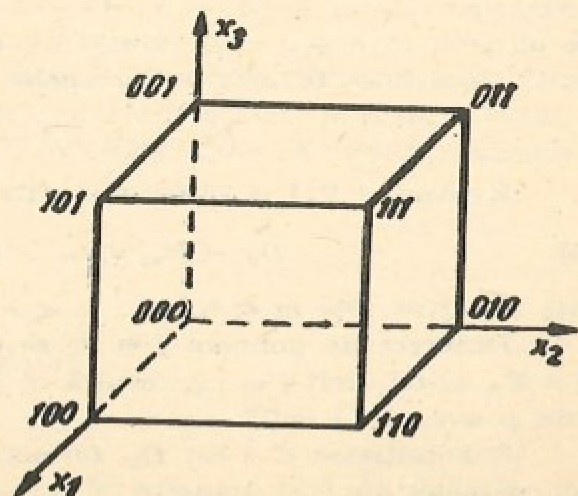


Fig. IV.3.

Să presupunem că dispunem de un *canal de transmisie* care constă dintr-un sistem care permite să se vehiculeze secvențe de două semnale, materializate în două nivele ale unui fenomen fizic (de exemplu tensiunea unei surse electrice), nivele pe care le punem în corespondență cu simbolurile 0 și 1.

Datorită „*zgomotului*" canalului de transmisie, cauzat de instabilitatea celor două nivele ale fenomenului fizic folosit, se poate recepţiona 0 în loc de 1 sau 1 în loc de 0. Dacă în transmisia unui cuvînt $x \in D_n$ se fac r erori, atunci cuvîntul recepţionat $y \in D_n$ se află la distanţa Hamming r de cuvîntul x (în r poziţii s-a recepţionat 0 în loc de 1 sau 1 în loc de 0). Se pune problema detectării cuvintelor recepţionate y care conţin erori şi, dacă este posibil, să corectăm erorile conţinute. O asemenea problematică face obiectul unei discipline relativ recente, cunoscută sub numele de *teoria codurilor*. Folosindu-se rezultate din teoria corpurilor finite au fost concepute numeroase *coduri detectoare şi coduri corectoare de erori*.

Pentru a simplifica prezentarea, să presupunem că trebuie să transmitem un mesaj x dintr-o mulţime de 2^m mesaje date prin cuvintele de lungime m peste alfabetul $A = \{0, 1\}$. Dacă cuvîntul recepţionat $y \in D_m$ conţine erori, avem $x \neq y$ şi deci y corespunde la un mesaj diferit de cel pe care am dorit să-l transmitem. O modalitate de a înlătura acest inconvenient este descrisă mai jos.

Să presupunem că pentru un număr $n > m$ se poate găsi o submulţime C a lui D_n astfel încît

$$|C| = 2^m \text{ şi } \mathrm{d}(u, v) \geqslant t + 1, \ \forall\, u, v \in C, \ u \neq v.$$

Cum $|C| = 2^m$ putem alege o bijecţie $c: D_m \to C$ prin care *codificăm* mesajele date prin cuvintele din D_m cu cuvinte de lungime n din C. Mulţimea C se numeşte *cod*, iar elementele sale *cuvinte-cod*.

Fie $x \in C$ un cuvînt cod şi fie $y \in D_n$ cuvîntul recepţionat corespunzător. Dacă în transmisia lui x s-au făcut cel mult t erori, atunci $\mathrm{d}(x, y) \leqslant t$. Avem $y \notin C$ şi deci y poate fi detectat. În adevăr, dacă $y \in C$ atunci $t + 1 \leqslant \mathrm{d}(x, y) \leqslant t$. Contradicţie.

Mai mult, dacă $\mathrm{d}(u, v) \geqslant 2t + 1$, $\forall\, u, v \in C$, $u \neq v$, atunci y poate fi chiar corectat. În adevăr, în aceste condiţii x este unicul cuvînt-cod care satisface $\mathrm{d}(x, y) \leqslant t$, căci dacă pentru $x' \in C$, $x' \neq x$, avem de asemenea $\mathrm{d}(x', y) \leqslant t$, atunci

$$2t + 1 \leqslant \mathrm{d}(x, x') \leqslant \mathrm{d}(x, y) + \mathrm{d}(y, x') \leqslant t + t = 2t.$$

Contradicţie.

În cazul codurilor polinomiale codificarea mesajelor precum şi recunoaşterea cuvintelor-cod se realizează prin prelucrări algebrice simple ale cuvintelor peste alfabetul $A = \{0, 1\}$.

Pentru a simplifica scrierea, vom nota elementele corpului $\mathbf{Z}_2$ cu 0 şi 1. Cu această convenţie de notaţie, operaţiile corpului $\mathbf{Z}_2$ sînt

$$\begin{array}{c|cc} + & 0 & 1 \\ \hline 0 & 0 & 1 \\ 1 & 1 & 0 \end{array}, \qquad \begin{array}{c|cc} \cdot & 0 & 1 \\ \hline 0 & 0 & 0 \\ 1 & 0 & 1 \end{array}$$

Se observă că $a + a = 0$, $\forall\, a \in \mathbf{Z}_2$, de unde rezultă că $f + f = 0$, $\forall\, f \in \mathbf{Z}_2[X]$. Să notăm cu P_n mulţimea tuturor polinoamelor $f \in \mathbf{Z}_2[X]$ de grad mai mic ca n.

$$f = a_0 + a_1X + \ldots + a_{n-1}X^{n-1}, \ (a_i \in \mathbf{Z}_2).$$

Evident, $|P_n| = 2^n$ iar aplicaţia

$$(*) \qquad D_n \to P_n, \ a_0a_1, \ldots, a_{n-1} \to a_0 + a_1X + \ldots + a_{n-1}X^{n-1}$$

este bijectivă. Fie $m \in \mathbf{N}$, $0 < m < n$ şi fie $p \in \mathbf{Z}_2[X]$ un polinom de grad $n - m$.

Deoarece un polinom $f \in P_n$ se divide prin p dacă şi numai dacă există un polinom $q \in P_m$ astfel încît $f = pq$, rezultă că pentru mulţimea $\mathcal{C}$ a polinoamelor din P_n care se divid prin p avem $|\mathcal{C}| = 2^m$.

Submulţimea C a lui D_n, formată cu cuvintele din D_n care prin bijecţia $(*)$ corespund polinoamelor din $\mathcal{C}$ se numeşte (n, m) — *codul polinoamelor* generat de p. Dacă $f \in \mathcal{C}$, atunci f se numeşte *polinom-cod*.

Aşa cum s-a observat, capacitatea unui cod de a detecta şi corecta erori este dată de distanţa minimă dintre cuvintele-cod. Prin alegerea adecvată a polinomului p pot fi obţinute coduri polinomiale cu bune performanţe în detectarea şi corectarea erorilor.

Fie, de asemenea, bijecţia

$$(**) \qquad D_m \to P_m,\ b_0b_1, \ldots, b_{m-1} \to b_0 + b_1X + \ldots + b_{m-1}X^{m-1}.$$

Dacă $g \in P_m$, atunci g este numit *polinom-mesaj*.

Există q, $r \in \mathbb{Z}_2[X]$ unic determinaţi astfel încît

$$X^{n-m}g = pq + r,\ r \in P_{n-m}.$$

Presupunem că $r = c_0 + c_1X + \ldots + c_{n-m-1}X^{n-m-1}$, $c_i \in \mathbb{Z}_2$, şi fie

$$f = r + X^{n-m}g = c_0 + c_1X + \ldots + c_{n-m-1}X^{n-m-1} + b_0X^{n-m} + \ldots + b_{m-1}X^{n-1}.$$

Avem $f \in \mathcal{C}$. În adevăr, cum $r + r = 0$, rezultă

$$f = r + X^{n-m}g = r + pq + r = pq.$$

Se observă că corespondenţa $P_m \to \mathcal{C}$, $g \to f$ realizată mai sus este bijectivă. Aşadar, de la mesaje la cuvintele-cod se trece astfel: mesajul $b_0b_1, \ldots, b_{m-1}$ trece prin bijecţia (**) în polinomul-mesaj $g = b_0 + b_1X + \ldots + b_{m-1}X^{m-1}$ căruia îi corespunde polinomul-cod $f = c_0 + c_1X + \ldots + c_{n-m-1}X^{n-m-1} + b_0X^{n-m} + \ldots + b_{m-1}X^{n-1}$, unde $r = c_0 + c_1X + \ldots$ $\ldots + c_{n-m-1}X^{n-m-1}$ este restul împărţirii lui $X^{n-m}g$ prin p. În fine, polinomul-cod f trece prin inversa bijecţiei (*) în cuvîntul-cod $c_0c_1 \ldots c_{n-m-1}b_0b_1, \ldots, b_{m-1}$. Evident, un cuvînt $x \in D_n$, $x = a_0a_1 \ldots a_{n-1}$ este în C dacă şi numai dacă polinomul $a_0 + a_1X + \ldots + a_{n-1}X^{n-1}$ se divide prin p.

Exerciţiu. Fie C (6, 3) — codul polinomului generat de polinomul $p = 1 + X + X^3 \in \mathbb{Z}_2[X]$.

1) Să se codifice mesajul 110;

2) Care dintre cuvintele 111001 şi 110011 sînt cuvinte-cod?

3) Arătaţi că orice cuvînt recepţionat y care conţine cel mult două erori poate fi detectat şi poate fi corectat dacă conţine numai o eroare.

Soluţie. 1) Mesajului 110 îi corespunde prin (**) polinomul-mesaj $g = 1 + X$, deci $X^{n-m}g = X^{6-3}(1 + X) = X^3 + X^4$. Făcînd împărţirea cu rest a polinomului $X^3 + X^4$ prin polinomul $p = 1 + X + X^3$ în inelul $\mathbb{Z}_2[X]$ se obţine restul $r = 1 + X^2$. Aşadar, polinomul-cod corespunzător lui $g = 1 + X$ este

$$f = r + X^3g = 1 + X^2 + X^3 + X^4.$$

căruia îi corespunde cuvîntul-cod 101110.

2) Cuvîntului 111001 din D_6 îi corespunde prin (*) polinomul $f = 1 + X + X^2 + X^5$. Se constată că p divide f, deci 111001 este cuvînt-cod.

Cuvîntului 110011 îi corespunde prin (*) polinomul $f = 1 + X + X^4 + X^5$ care împărţit la p dă restul X. Aşadar, p nu divide f, deci 110011 nu este cuvînt-cod.

3) Mesajele în (6, 3)-codul polinomial sînt cuvintele din D_3, deci 000, 100, 010, 001, 110, 101, 011, 111. Procedind ca la pct. 1) cuvintele-cod corespunzătoare sînt 000000, 110100, 011010, 111001, 101110, 001101, 100011, 010111. Cum $|C| = 8$ prin $C_8^2 = 28$ verificări directe se constată că $d(u, v) \geq 3 = 2 \times 1 + 1$, $\forall u, v \in C$, $u \neq v$.

Exerciţii

1. Pe mulţimea $A = \mathbb{Z} \times \mathbb{Z}$ definim legile de compoziţie:

$$(a, b) + (c, d) \stackrel{\text{def}}{=} (a + c, b + d)$$

$$(a, b)(c, d) \stackrel{\text{def}}{=} (ac + 3bd, ad + bc).$$

Arătați că aceste legi de compoziție conferă mulțimii A o structură de inel comutativ și fără divizori ai lui zero.

2. Pe mulțimea $\mathbf{Z}$ a numerelor întregi definim legile de compoziție :

$$x \perp y \overset{\text{def}}{=} x + y + 3, \qquad \forall x, y \in \mathbf{Z}$$

$$x \top y \overset{\text{def}}{=} xy + 3x + 3y + 6, \qquad \forall x, y \in \mathbf{Z}.$$

Arătați că :

1) $(\mathbf{Z}, \perp)$ este grup abelian.

2) $(\mathbf{Z}, \top)$ este monoid comutativ.

3) $x \top (y \perp z) = (x \top y) \perp (x \top z), \qquad \forall x, y, z \in \mathbf{Z}.$

Deduceți că $(\mathbf{Z}, \perp, \top)$ este inel comutativ fără divizori ai lui zero. Determinați elementele inversabile ale acestui inel.

3. Fie $a \in \mathbf{Z}$ și $f : \mathbf{Z} \to \mathbf{Z}$, $f(x) = x - a$, $\forall x \in \mathbf{Z}$.

1) Arătați că se pot defini în mod unic două legi de compoziție „$\perp$" și „$\top$" pe $\mathbf{Z}$ astfel încît :

$$f(x + y) = f(x) \perp f(y), \qquad \forall x, y \in \mathbf{Z}$$

$$f(xy) = f(x) \top f(y), \qquad \forall x, y \in \mathbf{Z}.$$

2) Arătați că $(\mathbf{Z}, \perp, \top)$ este inel comutativ și fără divizori ai lui zero, elementele sale inversabile fiind $1 - a$, $-1 - a$.

3) Cînd $a = 3$, comparați rezultatul cu cel de la Ex. 2.

4. Fie

$$A = \left\{ \begin{pmatrix} a & b \\ 5b & a \end{pmatrix} \middle| \ a, b \in \mathbf{Z} \right\}.$$

Arătați că A este o parte stabilă a lui $M_2(\mathbf{Z})$ în raport cu adunarea și înmulțirea matricelor și că formează inel comutativ și fără divizori ai lui zero în raport cu operațiile induse.

5. Pe mulțimea $A = \mathbf{Z} \times \mathbf{Z}$ definim legile de compoziție :

$$(a, b) + (c, d) \overset{\text{def}}{=} (a + c, b + d),$$

$$(a, b)\,(c, d) \overset{\text{def}}{=} (ac, bd).$$

Arătați că aceste legi de compoziție conferă mulțimii A o structură de inel comutativ cu divizori ai lui zero. Care sînt elementele inversabile ale acestui inel ?

6. Fie A_1 și A_2 două inele. Pe mulțimea $A = A_1 \times A_2$ definim legile de compoziție :

$$(a_1, a_2) + (b_1, b_2) \overset{\text{def}}{=} (a_1 + b_1, a_2 + b_2),$$

$$(a_1, a_2)\,(b_1, b_2) \overset{\text{def}}{=} (a_1 b_1, a_2 b_2).$$

1) Arătați că A are o structură de inel în raport cu aceste legi de compoziție (A este numit *produsul direct* al lui A_1 cu A_2).

2) Arătați că A este comutativ dacă și numai dacă A_1 și A_2 sînt inele comutative.

7. Fie $(\mathcal{R}_9, \oplus, \otimes)$ inelul resturilor modulo 9 și $A = \mathcal{R}_9 \times \mathbf{Z}$ produsul direct al inelului $\mathcal{R}_9$ cu inelul $\mathbf{Z}$ (v. Ex. 6).

1) Enumerați elementele inversabile ale inelului A.

2) Cum pot fi caracterizate elementele inversabile ale produsului direct a două inele ?

8. Fie $(\mathcal{R}_2, \oplus, \otimes)$ inelul resturilor modulo 2 și $B = \mathcal{R}_2 \times \mathcal{R}_2$ produsul direct al inelului $\mathcal{R}_2$ cu $\mathcal{R}_2$.

1) Alcătuiți tabla adunării și tabla înmulțirii inelului B.

2) Deduceți că $x + x = 0$ și $x^2 = x$, $\forall x = (x_1, x_2) \in B$.

9. Fie B un inel astfel încît $x^2 = x$, $\forall x \in B$. Arătaţi că:

1) $x + x = 0$, $\quad \forall x \in B$.
2) $xy = yx$, $\quad \forall x, y \in B$.

10. Arătaţi că într-un inel comutativ A avem:

$$a^n - b^n = (a - b)(a^{n-1} + a^{n-2}b + \ldots + b^{n-1}), \ \forall a, b \in A.$$

11. Arătaţi că într-un inel comutativ A este valabilă formula binomului lui Newton

$$(a + b)^n = \sum_{k=0}^{n} C_n^k a^{n-k} b^k, \ \forall a, b \in A.$$

12. Fie $(\mathcal{R}_5, \oplus, \otimes)$ inelul resturilor modulo 5.

1) Verificaţi că $a \oplus a \oplus a \oplus a \oplus a = 0$, $\forall a \in \mathcal{R}$.
2) Deduceţi, folosind formula binomului lui Newton, că

$$(a \oplus b)^5 = a^5 \oplus b^5 \qquad \forall a, b \in \mathcal{R}_5.$$

13. Fie $U \in M_3(\mathbf{R})$,

$$U = \begin{pmatrix} 0 & a & b \\ 0 & 0 & c \\ 0 & 0 & 0 \end{pmatrix} \ a, b, c \in \mathbf{R}.$$

1) Pentru ce numere $a, b, c \in \mathbf{R}$ avem $U^2 = 0$?
2) Dacă $U^2 = 0$, atunci $E - U$ este inversabilă şi $(E - U)^{-1} = E + U$.

14. Fie $\mathbf{Z}_{12}$ inelul claselor de resturi modulo 12 şi G mulţimea elementelor inversabile ale acestui inel.

1) Determinaţi elementele lui G şi arătaţi că G este o parte stabilă în raport cu înmulţirea lui $\mathbf{Z}_{12}$.
2) Alcătuiţi tabla operaţiei induse şi deduceţi că $(G, \cdot)$ este grup izomorf cu grupul lui Klein.

15. Rezolvaţi următorul sistem de ecuaţii liniare cu coeficienţi în inelul $\mathbf{Z}_{12}$:

$$\begin{cases} \hat{3}x + \hat{2}y = \hat{4}, \\ \hat{2}x + \hat{3}y = \hat{1}. \end{cases}$$

16. Fie $U \in M_2(\mathbf{Z}_{12})$, $U = \begin{pmatrix} \hat{a} & \hat{b} \\ \hat{c} & \hat{d} \end{pmatrix}$ şi $\hat{e} = \hat{a}\hat{d} - \hat{c}\hat{b} = \det(U)$.

1) Arătaţi că matricea U este element inversabil al inelului $M_2(\mathbf{Z}_{12})$ dacă şi numai dacă $\det(U)$ este egal cu $\hat{1}$, $\hat{5}$, $\hat{7}$ sau $\hat{11}$ şi

$$U^{-1} = \hat{e}^{-1} \begin{pmatrix} \hat{d} & -\hat{b} \\ -\hat{c} & \hat{a} \end{pmatrix}.$$

2) Următoarele matrice din $M_2(\mathbf{Z}_{12})$ sînt inversabile şi găsiţi inversele lor:

$$U = \begin{pmatrix} \hat{2} & \hat{1} \\ \hat{1} & \hat{3} \end{pmatrix}, \qquad V = \begin{pmatrix} \hat{5} & \hat{4} \\ \hat{1} & \hat{3} \end{pmatrix}, \qquad W = \begin{pmatrix} \hat{2} & \hat{1} \\ \hat{1} & \hat{1} \end{pmatrix}.$$

17. Pe mulţimea $K = \mathbf{Q} \times \mathbf{Q}$ definim legile de compoziţie :

$$(a, b) + (c, d) = (a + c, b + d),$$
$$(a, b)(c, d) = (ac - bd, ad + bc + bd).$$

Arătaţi că aceste operaţii conferă lui K o structură de corp comutativ.

18. Pe mulţimea $K = \mathbf{R} \times \mathbf{R}$ definim legile de compoziţie :

$$(a, b) + (c, d) = (a + c, b + d),$$
$$(a, b)(c, d) = (ac - bd, ad + bc).$$

Arătaţi că aceste operaţii conferă mulţimii K o structură de corp comutativ.

19. Pe intervalul $K = (0, \infty)$ definim legile de compoziţie :

$$x \perp y = xy, \qquad \forall\, x, y \in K,$$
$$x \top y = x^{\ln y}, \qquad \forall\, x, y \in K.$$

Arătaţi că tripletul $(K, \perp, \top)$ este un corp comutativ.

20. Fie $L = \left\{ \begin{pmatrix} \hat{a} & \hat{b} \\ -\hat{b} & \hat{a} \end{pmatrix} \middle| a, b \in \mathbf{Z}_3 \right\}$.

1) Arătaţi că $\hat{x}^2 + \hat{y}^2 \neq \hat{0}$, $\quad \forall\, \hat{x}, \hat{y} \in \mathbf{Z}_3$, $\hat{x} \neq \hat{0}$ sau $\hat{y} \neq \hat{0}$.

2) Arătaţi că L este o parte stabilă a lui $M_2(\mathbf{Z}_3)$ în raport cu adunarea şi înmulţirea şi că formează corp comutativ cu 9 elemente faţă de operaţiile induse.

21. Pe mulţimea $A = \mathbf{Z} \times \mathbf{Z}$ definim legile de compoziţie :

$$(a, b) + (c, d) = (a + c, b + d),$$
$$(a, b)(c, d) = (ac - bd, ad + bc).$$

1) Arătaţi că A are o structură de inel comutativ în raport cu aceste legi de compoziţie.

2) Determinaţi elementele inversabile ale inelului A.

3) Arătaţi că $A \simeq \mathbf{Z}[i]$.

22. Arătaţi că funcţia $f : \mathbf{Q}(\sqrt{-3}) \to K$

$f(z) = (a - b, 2b)$, $z \in \mathbf{Q}(\sqrt{-3})$, $z = a + b\sqrt{-3}$ cu $a, b \in \mathbf{Q}$ este un izomorfism de la corpul $\mathbf{Q}(\sqrt{-3})$ la corpul K de la Ex. 17.

23. Arătaţi că corpul $\mathbf{C}$ este izomorf cu corpul K de la Ex. 18.

24. Arătaţi că corpul $\mathbf{R}$ este izomorf cu corpul K de la Ex. 19.

25. Fie $K = \left\{ \begin{pmatrix} a & 2b \\ b & a \end{pmatrix} \middle| a, b \in \mathbf{Q} \right\}$.

1) Arătaţi că mulţimea K este o parte stabilă a lui $M_2(\mathbf{Q})$ în raport cu adunarea şi înmulţirea şi că formează corp în raport cu operaţiile induse.

2) Arătaţi că $\mathbf{Q}(\sqrt{2}) \simeq K$.

26. Fie $a, b, c \in \mathbf{R}$. Pe $\mathbf{R}$ definim legile de compoziţie :

$$x \perp y = ax + by - 2, \qquad \forall\, x, y \in \mathbf{R},$$
$$x \top y = xy - 2x - 2y + c, \qquad \forall\, x, y \in \mathbf{R}.$$

1) Determinaţi a, b, c astfel încît $(\mathbf{R}, \perp, \top)$ să fie corp.

2) Determinați apoi $\alpha, \beta \in \mathbf{R}$ astfel încît funcția :

$$f: \mathbf{R} \to \mathbf{R},\ f(x) = \alpha x + \beta, \quad \forall\ x \in \mathbf{R}$$

să stabilească un izomorfism de la corpul $(\mathbf{R}, +, \cdot)$ al numerelor reale la corpul $(\mathbf{R}, \perp, \top)$.

27. Fie $f, g \in \mathbf{Z}_5[X]$, $f = \hat{2}X^3 + \hat{4}X^2 + \hat{3}X + \hat{1}$ și $g = \hat{3}X^3 + \hat{2}X^2 + X + \hat{3}$. Calculați $f + g$ și fg.

28. Fie $f, g \in \mathbf{Z}_6[X]$, $f = \hat{3}X^2 + \hat{3}X + \hat{3}$, $g = \hat{2}X^3 + \hat{4}X + \hat{2}$. Calculați fg.

29. Fie $f \in \mathbf{Z}_3[X]$, $f = X^3 + \hat{2}X^2 + X + \hat{1}$. Determinați toate polinoamele $g = aX^3 + bX^2 + cX + d \in \mathbf{Z}_3[X]$ cu proprietatea : $\overline{g} = \overline{f}$.

30. Enumerați rădăcinile din $\mathbf{Z}_6$ ale polinomului $f = \hat{3}X^2 + \hat{3}X \in \mathbf{Z}_6[X]$.

31. Să se determine două polinoame f și g de grad 1, $f, g \in \mathbf{Q}[X]$, astfel încît

$$f^2 + g^2 = X^2 + 1,\ f(2)g(2) = 2.$$

32. Determinați gradul polinomului $f \in \mathbf{R}[X]$,

$$f = (\lambda^2 + 3\lambda + 2)X^3 + (\lambda^2 + 4\lambda + 3)X^2 + (\lambda^2 - 1)X + 1, \text{ unde}$$

λ este un parametru real.

33. Să se determine două polinoame f și g de grad 1, $f, g \in \mathbf{Z}[X]$, astfel încît

$$(X^2 + 2X + 2)f + (X^2 + 3X + 3)g = 1.$$

34. Fie K un corp comutativ și $f_1, f_2, f_3 \in K[X]$, grad $f_i = i$, $1 \leqslant i \leqslant 3$. Arătați că egalitatea

$$\alpha_1 f_1 + \alpha_2 f_2 + \alpha_3 f_3 = 0 \ (\alpha_i \in K)$$

este posibilă numai în cazul $\alpha_1 = \alpha_2 = \alpha_3 = 0$. Generalizare.

35. Fie $f \in \mathbf{R}[X]$, grad $f \leqslant 2$. Dacă există trei numere reale diferite $\alpha_1, \alpha_2, \alpha_3$ astfel încît

$$f(\alpha_i) = 0,\ i = 1, 2, 3,$$

atunci f este egal cu polinomul zero. Generalizare.

36. Fie $f, g \in \mathbf{Z}_5[X]$, $f = \hat{3}X^5 + X^3 + \hat{2}X + \hat{4}$, $g = \hat{2}X^3 + \hat{3}X^2 + \hat{1}$. Aflați cîtul și restul împărțirii lui f prin g.

37. Fie $f, g \in \mathbf{Q}[X]$, $f = 2X^4 - 3X^2 + aX + b$, $g = X^2 - 2X + 3$. Să se determine a și b astfel încît $g \mid f$.

38. Fie $f \in \mathbf{Z}[X]$, $f = a_0 + a_1X + a_2X^2 + a_3X^3$. Determinați coeficienții polinomului f dacă

$$f(1) + f(2) + \ldots + f(n) = n^4,\ \forall\ n > 0$$

39. Fie $f \in \mathbf{C}[X]$, $f = a + bX + X^2$. Determinați a și b astfel încît f să dividă polinomul $X^4 + 1$.

40. Fie $f \in \mathbf{Q}[X]$, $f = X^5 - 5X^4 + 18X^3 - 15X^2 + X + 4$. Folosind schema lui Horner, calculați $f(3)$.

41. Calculați cu schema lui Horner cîtul și restul împărțirii polinomului

$$f \in \mathbf{Z}_7[X],\ f = \hat{5}X^4 + \hat{3}X^2 + X + \hat{2}, \text{ prin } X + \hat{5}.$$

42. Dacă polinomul $f \in \mathbf{Z}[X]$ admite două rădăcini întregi de parități diferite, atunci $f(k)$ este par, $\forall\ k \in \mathbf{Z}$.

43. Să se descompună în factori ireductibili peste $\mathbf{R}$ și peste $\mathbf{C}$ polinoamele $X^4 + 4$, $X^6 + 27$.

44. Să se descompună în factori ireductibili peste $\mathbf{Z}_5$ polinomul

$$f = X^4 + X^3 + \hat{2}X^2 + X + \hat{1}.$$

45. Fie $f \in \mathbf{Q}[X]$, $f = X^3 - 2$.
1) Arătați că f este ireductibil peste $\mathbf{Q}$.
2) Descompuneți în factori ireductibili polinomul f peste $\mathbf{R}$ și peste $\mathbf{C}$.

46*. Fie $A = \{0, 1, a, b\}$ un inel cu 4 elemente. Arătați că :
1) Funcția $f: A \to A$, $f(x) = 1 + x$, $\forall\, x \in A$ este bijectivă.
2) $\sum\limits_{x \in A} f(x) = 1 + a + b$ și $1 + 1 + 1 + 1 = 0$ ·
3) Dacă A este corp, atunci $1 + 1 = 0$

47*. Fie $A = \{0, 1, a, b)$ un inel cu patru elemente. Afirmațiile următoare sînt echivalente :
i) A este corp ;
ii) Există $x \in A$ astfel încît $1 + x = x^2$.

48*. Fie A un inel astfel încît $x^6 = x$, $\forall x \in A$. Arătați că $x^2 = x$, $\forall x \in A$.

49*. Fie A mulțimea tuturor funcțiilor continue $f: [0, 1] \to \mathbf{R}$.
1) Arătați că A este inel comutativ în raport cu adunarea și înmulțirea funcțiilor reale de variabilă reală ;
2) Pentru $f \in A$, $f \neq 0$ există $g \in A$, $g \neq 0$ astfel încît $fg = 0$, dacă și numai dacă mulțimea $\{x \mid f(x) = 0\}$ conține un interval :
3) Determinați funcțiile din A cu proprietatea $f^2 = f$.

50*. Dacă $f: \mathbf{Q} \to \mathbf{C}$ este un morfism de corpuri, atunci $f(x) = x$, $\forall x \in \mathbf{Q}$. Determinați apoi automorfismele corpului $\mathbf{Q}(\sqrt{2})$.

51*. Fie $\mathbf{R}$ corpul numerelor reale și $f: \mathbf{R} \to \mathbf{R}$ un morfism de corpuri. Arătați că $f = 1_{\mathbf{R}}$.

52*. Fie $f, g \in \mathbf{Z}[X]$, $h = fg$ și $p > 0$ un număr prim. Dacă toți coeficienții lui h se divid prin p atunci cel puțin unul din polinoamele f, g are toți coeficienții divizibili prin p.

53*. Descompuneți în produs de polinoame ireductibile peste corpul $\mathbf{Z}_2$ polinoamele de grad $\leqslant 4$ din $\mathbf{Z}_2[X]$.

54*. Fie L și L' două pătrate latine ortogonale de ordin n peste mulțimea $M = \{0, 1, 2, \ldots, n - 1\}$ astfel încît suma numerelor de pe fiecare diagonală a lui L și fiecare diagonală a lui L' este $n(n - 1)/2$. Fie $a_{ij} = l_{ij}n + l'_{ij} + 1$, unde $l_{ij}(l'_{ij})$ este numărul de la intersecția liniei i cu coloana j din L (resp. L'). Arătați că matricea $U = (a_{ij}) \in M_n(\mathbf{Z})$ este *„magică"*, adică conține numerele de la 1 la n^2 și suma numerelor de pe fiecare linie (coloană, diagonală) este aceeași, anume $n(n^2 + 1)/2$.

55*. Construiți cîte o matrice „magică" ($\equiv$ *careu magic*) de ordin 3, 4 și 5, folosind corpuri cu 3, 4 și 5 elemente respectiv.

SPAȚII VECTORIALE

§ 1. LEGI DE COMPOZIȚIE EXTERNE

Legile de compoziție studiate în capitolele anterioare sînt aplicații de tipul

$$\varphi : M \times M \to M, \quad (x, y) \to \varphi(x, y) \in M,$$

unde M este o mulțime nevidă. Ele se numesc încă *legi de compoziție interne*.

Noțiunea de lege de compoziție internă este un caz particular al unui concept mai general :

1.1. *Definiție.* **Fie Ω și M două mulțimi nevide. O aplicație**

$$\psi : \Omega \times M \to M, \quad (\omega, x) \to \psi(\omega, x) \in M$$

se numește *lege de compoziție externă* **pe M cu** *operatori* **în Ω.**

Pentru *compusul* $\psi(\omega, x)$ al elementului $x \in M$ cu *operatorul* $\omega \in \Omega$ se folosește de regulă notația multiplicativă, $\psi(\omega, x) = \omega x$. Mulțimea Ω poartă numele de *domeniul operatorilor legii* de compoziție externe ψ. O lege de compoziție internă pe M poate fi privită ca o lege de compoziție externă cu domeniul operatorilor $\Omega = M$.

Exemple

1. *Înmulțirea matricelor cu scalari.* Fie $\Omega = \mathbf{R}$ și $M = M_2(\mathbf{R})$. Pentru orice $\alpha \in \mathbf{R}$ și $A \in M_2(\mathbf{R})$, $A = (a_{ij})$ definim matricea $\alpha A \in M_2(\mathbf{R})$,

$$\alpha A \stackrel{\text{def}}{=} \begin{pmatrix} \alpha a_{11} & \alpha a_{12} \\ \alpha a_{21} & \alpha a_{22} \end{pmatrix}.$$

Se obține astfel o lege de compoziție externă pe $M_2(\mathbf{R})$ cu operatori în $\mathbf{R}$

$$\mathbf{R} \times M_2(\mathbf{R}) \to M_2(\mathbf{R}), \ (\alpha, A) \to \alpha A,$$

numită *înmulțirea matricelor cu scalari*.

Operațiile de adunare și înmulțire ale corpului $\mathbf{R}$, adunarea matricelor din $M_2(\mathbf{R})$ și înmulțirea matricelor cu scalari sînt legate prin :

$$S_1)\ (\alpha + \beta)A = \alpha A + \beta A,$$

$$S_2)\ \alpha(A + B) = \alpha A + \alpha B,$$

$$S_3)\ \alpha(\beta A) = (\alpha\beta)A,$$

$$S_4)\ 1 \cdot A = A$$

oricare ar fi $\alpha, \beta \in \mathbf{R}$ și $A, B \in M_2(\mathbf{R})$.

Pentru exemplificare, să demonstrăm S_3. Avem :

$$\alpha(\beta A) = \alpha\begin{pmatrix}\beta a_{11} & \beta a_{12}\\ \beta a_{21} & \beta a_{22}\end{pmatrix} = \begin{pmatrix}\alpha(\beta a_{12}) & \alpha(\beta a_{11})\\ \alpha(\beta a_{21}) & \alpha(\beta a_{22})\end{pmatrix} = \begin{pmatrix}(\alpha\beta)a_{11} & (\alpha\beta)a_{12}\\ (\alpha\beta)a_{21} & (\alpha\beta)a_{22}\end{pmatrix} = (\alpha\beta)A.$$

2. *Înmulţirea polinoamelor cu scalari*. Fie $\Omega = \mathbf{R}$ şi $M = \mathbf{R}[X]$. Pentru orice $\alpha \in \mathbf{R}$ şi $f \in \mathbf{R}[X]$, $f = a_0 + a_1X + \ldots + a_mX^m$, definim polinomul $\alpha f \in \mathbf{R}[X]$,

$$\alpha f \overset{\text{def}}{=} \alpha a_0 + \alpha a_1 X + \ldots + \alpha a_m X^m.$$

Se obţine astfel o lege de compoziţie externă pe $\mathbf{R}[X]$ cu operatori în $\mathbf{R}$,

$$\mathbf{R} \times \mathbf{R}[X] \to \mathbf{R}[X],\ (\alpha, f) \to \alpha f,$$

numită *înmulţirea polinoamelor cu scalari*.

Înmulţirea polinoamelor cu scalari are proprietăţile :

$S_1)$ $(\alpha + \beta)f = \alpha f + \beta f$,

$S_2)$ $\alpha(f + g) = \alpha f + \alpha g$,

$S_3)$ $\alpha(\beta f) = (\alpha\beta)f$,

$S_4)$ $1 \cdot f = f$

oricare ar fi $\alpha, \beta \in \mathbf{R}$ şi $f, g \in \mathbf{R}[X]$. Astfel :

$S_1)$
$$(\alpha + \beta)f = (\alpha + \beta)a_0 + (\alpha + \beta)a_1X + \ldots + (\alpha + \beta)a_mX^m =$$
$$= \alpha a_0 + \beta a_0 + \alpha a_1 X + \beta a_1 X + \ldots + \alpha a_m X^m + \beta a_m X^m =$$
$$= \alpha a_0 + \alpha a_1 X + \ldots + \alpha a_m X^m + \beta a_0 + \beta a_1 X + \ldots + \beta a_m X^m = \alpha f + \beta f.$$

3. *Înmulţirea vectorilor de poziţie cu scalari*. Fie Π un plan euclidian în care fixăm un punct O ce va fi numit *origine*. Fiecărui punct P al planului Π i se asociază segmentul orientat x cu originea în O şi extremitatea în P, numit *vectorul de poziţie* al punctului P (relativ la originea O).

Să notăm cu V mulţimea tuturor vectorilor de poziţie astfel obţinuţi. Dacă $x, y \in V$, se notează cu $x + y$ vectorul de poziţie al celui de-al patrulea vîrf al paralelogramului determinat de x şi y (v. fig. V.1). Se obţine astfel o lege de compoziţie internă pe V,

$$V \times V \to V,\quad (x, y) \Rightarrow x + y,$$

numită *adunarea geometrică* a vectorilor de poziţie. Procedeul descris mai sus de aflare a sumei geometrice a doi vectori de poziţie este cunoscut sub numele de *„regula paralelogramului"*. Consideraţii geometrice simple arată că $(V, +)$ este grup abelian ; elementul neutru al acestui grup este vectorul de poziţie al originii O, iar opusul lui x este vectorul de poziţie al simetricului lui P în raport cu O (v. fig. V.1).

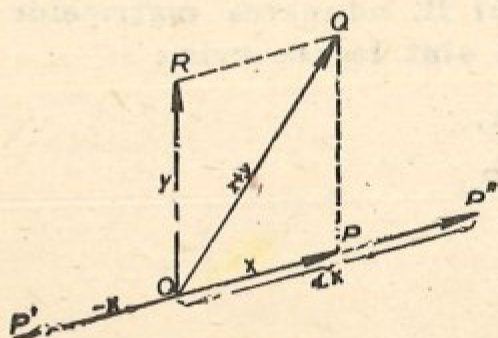


Fig. V.1.

Dacă α este un număr real, iar x este vectorul de poziţie al punctului P, atunci *produsul* lui α cu x, notat cu αx, este prin definiţie vectorul de poziţie al punctului P'' determinat prin condiţiile :

1) lungimea lui OP'' este egală cu produsul dintre $|\alpha|$ și lungimea lui OP;

2) P'' se găsește pe dreapta determinată de O și P de aceeași parte cu P față de O dacă $\alpha > 0$, în partea opusă cînd $\alpha < 0$.

Se obține astfel o lege de compoziție externă pe V cu operatori în $\mathbf{R}$,

$$\mathbf{R} \times V \to V, \quad (\alpha, x) \to \alpha x,$$

numită *înmulțirea vectorilor de poziție cu scalari.*

Această lege de compoziție are proprietățile:

$$S_1)\ (\alpha + \beta)x = \alpha x + \beta x,$$

$$S_2)\ \alpha(x + y) = \alpha x + \alpha y,$$

$$S_3)\ \alpha(\beta x) = (\alpha\beta)x,$$

$$S_4)\ 1 \cdot x = x$$

oricare ar fi $\alpha, \beta \in \mathbf{R}$ și $x, y \in V$.

§ 2. DEFINIȚIA SPAȚIULUI VECTORIAL

2.1. *Definiție.* **Fie K un corp. Se numește** *spațiu vectorial* **(peste corpul K) un grup abelian $(V, +)$ pe care este dată o lege de compoziție externă cu operatori în K,**

$$K \times V \to V, \quad (\alpha, u) \to \alpha u,$$

care satisface axiomele:

$$S_1)\ (\alpha + \beta)u = \alpha u + \beta u,$$

$$S_2)\ \alpha(u + v) = \alpha u + \alpha v,$$

$$S_3)\ \alpha(\beta u) = (\alpha\beta)u,$$

$$S_4)\ 1 \cdot u = u$$

oricare ar fi $\alpha, \beta \in K$, $u, v \in V$.

Se folosește următoarea terminologie:

— elementele lui V se numesc *vectori*, iar operația grupului $(V, +)$ se numește *adunarea vectorilor*;

— elementele lui K se numesc *scalari*, iar legea de compoziție externă $K \times V \to V$ se numește *înmulțirea vectorilor cu scalari*;

— elementul neutru al grupului $(V, +)$ se numește *vectorul zero*, notat cu 0, ca și scalarul zero;

— cînd $K = \mathbf{R}$ sau $K = \mathbf{C}$ se spune că V este *spațiul vectorial real*, respectiv *complex*;

— spațiile vectoriale se numesc încă *spații liniare*.

Să observăm că S_1 şi S_2 consemnează faptul că înmulţirea vectorilor cu scalari este distributivă faţă de adunarea scalarilor, respectiv adunarea vectorilor, iar S_3 descrie o lege de asociativitate care angajează atît înmulţirea vectorilor cu scalari cît şi înmulţirea scalarilor.

Notă. Iniţial noţiunea de vector a apărut în mecanică şi fizică, avînd ca model geometric segmentul orientat şi fiind folosit pentru a descrie mărimi caracterizate prin valoare numerică, direcţie şi sens. Ulterior, aria de aplicabilitate a noţiunii de vector s-a lărgit considerabil. Definiţia dată mai sus spaţiului vectorial dă posibilitatea de a pune în „postura" de vector obiecte de natură variată. De exemplu : matrice, funcţii şi polinoame în matematică, secvenţe finite de 0 şi 1 în teoria codurilor, sisteme ordonate $(x_1, x_2, \ldots, x_n)$ de numere reale în economie.

Exemple

1. *Spaţiul vectorial* $\mathbf{R}^n$. Fie $n > 1$ un număr natural. Se notează cu $\mathbf{R}^n$ mulţimea tuturor sistemelor ordonate de n numere reale,

$$x = (a_1, a_2, \ldots, a_n), \quad (a_i \in \mathbf{R}).$$

Dacă $\alpha \in \mathbf{R}$ şi $x, y \in \mathbf{R}^n$, $x = (a_1, a_2, \ldots, a_n)$, $y = (b_1, b_2, \ldots, b_n)$ atunci :

$$x = y \overset{\text{def}}{\Leftrightarrow} a_i = b_i\,;\ 1 \leqslant i \leqslant n,$$

$$x + y \overset{\text{def}}{=} (a_1 + b_1, a_2 + b_2, \ldots, a_n + b_n),$$

$$\alpha x \overset{\text{def}}{=} (\alpha a_1, \alpha a_2, \ldots, \alpha a_n).$$

O verificare directă arată că legea de compoziţie internă

$$\mathbf{R}^n \times \mathbf{R}^n \to \mathbf{R}^n, \ (x, y) \to x + y$$

este asociativă şi comutativă. Dacă $0 = (0, 0, \ldots, 0)$, atunci oricare ar fi $x \in \mathbf{R}^n$, $x = (a_1, a_2, \ldots, a_n)$ avem

$$0 + x = (0 + a_1, 0 + a_2, \ldots, 0 + a_n) = (a_1, a_2, \ldots, a_n) = x = x + 0,$$

iar dacă punem

$$-x = (-a_1, -a_2, \ldots, -a_n)$$

avem şi

$$x + (-x) = (a_1 + (-a_1), a_2 + (-a_2), \ldots, a_n + (-a_n)) = 0 = (-x) + x.$$

Rezultă că $(\mathbf{R}^n, +)$ este grup abelian.

De asemenea, se verifică că legea de compoziţie externă

$$\mathbf{R} \times \mathbf{R}^n \to \mathbf{R}^n, \quad (\alpha, x) \to \alpha x$$

satisface axiomele $S_1 - S_4$ din definiţia spaţiului vectorial. Astfel,

$$\forall \alpha \in \mathbf{R} \text{ şi } x, y \in \mathbf{R}^n, \ x = (a_1, a_2, \ldots, a_n),$$
$$y = (b_1, b_2, \ldots, b_n)$$

avem:

$$\alpha(x+y)=\alpha(a_1+b_1,\ a_2+b_2,\ \dots,\ a_n+b_n)=(\alpha(a_1+b_1),\ \alpha(a_2+b_2),\ \dots,\alpha(a_n+b_n))=(\alpha a_1+\alpha b_1,\alpha a_2+\alpha b_2,\dots,\alpha a_n+\alpha b_n)=(\alpha a_1,\alpha a_2,\dots,\alpha a_n)+(\alpha b_1,\ \alpha b_2,\ \dots,\ \alpha b_n)=\alpha x+\alpha y,$$

deci axioma S_2 este verificată.

Elementele lui $\mathbf{R}^n$ se numesc *vectori* (linie) *n-dimensionali* iar $\mathbf{R}^n$ se numeşte *spaţiul aritmetic real* de dimensiune n, sau *spaţiul vectorilor linie n-dimensionali*. Dacă $x \in \mathbf{R}^n$, $x=(a_1, a_2, \dots, a_n)$, atunci a_i se numeşte *componenta* de rang i a lui x, $1 \leqslant i \leqslant n$.

În unele aplicaţii este avantajos să dăm vectorii lui $\mathbf{R}^n$ sub formă de coloane,

$$x=\begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix} \quad (a_i \in \mathbf{R}).$$

În acest caz $\mathbf{R}^n$ va fi numit *spaţiul vectorilor coloană n-dimensionali*. Analog, se introduce spaţiul aritmetic $\mathbf{C}^n$ şi de asemenea spaţiul vectorial K^n, K corp oarecare.

2. Mulţimea $M_2(\mathbf{R})$ a matricelor pătratice de ordin 2 cu coeficienţi reali formează spaţiul vectorial peste corpul $\mathbf{R}$ în raport cu adunarea şi înmulţirea matricelor cu scalari. În adevăr, $(M_2(\mathbf{R}), +)$ este grup abelian, iar înmulţirea matricelor cu scalari satisface axiomele S_1—S_4 (v. § 1).
3. Mulţimea $\mathbf{R}[X]$ a polinoamelor în nedeterminata X cu coeficienţi reali formează spaţiu vectorial peste corpul $\mathbf{R}$ în raport cu adunarea şi înmulţirea polinoamelor cu scalari (v. § 1).
4. Mulţimea V a vectorilor de poziţie ai punctelor dintr-un plan cu originea într-un punct O a planului formează spaţiul vectorial peste corpul $\mathbf{R}$ în raport cu adunarea şi înmulţirea cu scalari (v. § 1).
5. *Spaţiul vectorial* 0. Fie K un corp. Pe grupul abelian zero, $0=\{0\}$, introducem legea de compoziţie externă

$$K \times 0 \to 0,\ (\alpha, 0) \to \alpha \cdot 0 = 0.$$

Se conferă astfel grupului abelian 0 o structură de spaţiu vectorial peste K, numit *spaţiul vectorial zero*.

Fie V un spaţiu vectorial peste corpul K. Cum $(V, +)$ este grup abelian, pentru adunarea vectorilor sînt valabile regulile de calcul dintr-un grup abelian. Să adaugăm la acestea următoarele proprietăţi specifice ale operaţiilor cu vectori:

a) Fie $\alpha \in K$ şi $x \in V$. Atunci:

$$\boxed{\alpha x = 0 \Leftrightarrow \alpha = 0 \text{ sau } x = 0}$$

În adevăr, fie $\alpha = 0$ și $y = 0 \cdot x$. Atunci

$$y = 0x = (0 + 0)x = 0x + 0x = y + y,$$

de unde

$$y = y + 0 = y + (y + (-y)) = (y + y) + (-y) = y + (-y) = 0,$$

deci $0x = 0$ și analog se arată că $\alpha x = 0$.

Reciproc, presupunem că $\alpha x = 0$. Dacă $\alpha \neq 0$, atunci

$$x = 1 \cdot x = (\alpha^{-1}\alpha)x = \alpha^{-1}(\alpha x) = \alpha^{-1}0 = 0.$$

b) Oricare ar fi $\alpha \in K$ și $x \in V$, avem :

$$\boxed{(-\alpha)x = \alpha(-x) = -\alpha x, \ (-\alpha)(-x) = \alpha x}.$$

În adevăr,

$$0 = \alpha 0 = \alpha(x + (-x)) = \alpha x + \alpha(-x),$$

de unde rezultă că $\alpha(-x)$ este opusul vectorului αx deci $\alpha(-x) = -\alpha x$. Analog se arată că $(-\alpha)x = -\alpha x$ și atunci

$$(-\alpha)(-x) = -(\alpha(-x)) = -(-\alpha x) = \alpha x.$$

c) Oricare ar fi $\alpha, \beta \in K$ și $x, y \in V$ avem :

$$\boxed{(\alpha - \beta)x = \alpha x - \beta x, \ \alpha(x - y) = \alpha x - \alpha y}.$$

În adevăr,

$$(\alpha - \beta)x = (\alpha + (-\beta))x = \alpha x + (-\beta)x = \alpha x - \beta x$$

și la fel se demonstrează a doua regulă de distributivitate.

§ 3. DEPENDENȚA ȘI INDEPENDENȚA LINIARA. BAZA. COORDONATE

1. **Bază.** a) Fie V spațiul vectorilor de poziție dintr-un plan euclidian. Fie v_1 și v_2 doi vectori de poziție diferiți de zero și necoliniari (v. fig. V.2).

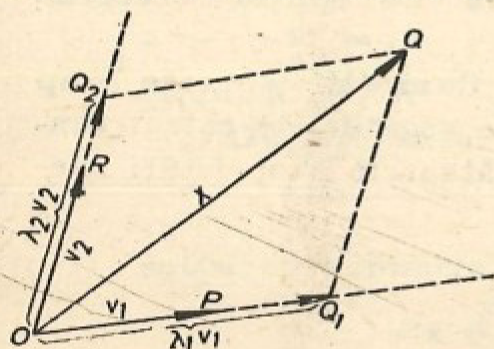


Fig. V.2.

Sistemul de vectori **B** format cu v_1 și v_2 $\mathbf{B} = (v_1, v_2)$ are proprietățile :

1) $\forall x \in V$, $\exists \lambda_1, \lambda_2 \in \mathbf{R}$ astfel încît $x = \lambda_1 v_1 + \lambda_2 v_2$,

2) Dacă $\alpha_1 v_1 + \alpha_2 v_2 = 0$, cu $\alpha_1, \alpha_2 \in \mathbf{R}$, atunci $\alpha_1 = \alpha_2 = 0$.

În adevăr, paralelele duse prin extremitatea Q a vectorului x la dreptele definite de v_1 și v_2 determină pe acestea punctele Q_1 și Q_2 respectiv. Există $\lambda_1, \lambda_2 \in \mathbf{R}$ astfel încît $QQ_1 = \lambda_1 v_1$ și

$QQ_2 = \lambda_2 v_2$. Din construcție rezultă că suma geometrică a vectorilor de poziție $\lambda_1 v_1$ și $\lambda_2 v_2$ este egală cu x, deci

$$x = \lambda_1 v_1 + \lambda_2 v_2$$

și 1) este astfel verificat. Dacă 2) nu este adevărat, există $\alpha_1, \alpha_2 \in \mathbf{R}$, $\alpha_1 \neq 0$ sau $\alpha_2 \neq 0$, astfel încît

$$\alpha_1 v_1 + \alpha_2 v_2 = 0.$$

Presupunem că $\alpha_1 \neq 0$. Atunci deducem că $v_1 = -\alpha^{-1}\alpha_2 v_2$, deci v_1 și v_2 sînt coliniari, contrar ipotezei.

b) În spațiul vectorial $\mathbf{R}^3$ să considerăm vectorii v_1, v_2, v_3, unde $v_1 = (1, 1, 1)$, $v_2 = (0, 1, 1)$ și $v_3 = (0, 0, 1)$ Fie $\mathbf{B}$ sistemul format cu v_1, v_2, v_3, $\mathbf{B} = (v_1, v_2, v_3)$. Vectorul zero al spațiului $\mathbf{R}^3$ este $(0, 0, 0)$ și va fi notat cu 0 ca și scalarul zero.

Sistemul de vectori $\mathbf{B}$ are proprietățile :

1) $\forall x \in \mathbf{R}^3$, $\exists \lambda_1, \lambda_2, \lambda_3 \in \mathbf{R}$ astfel încît

$$x = \lambda_1 v_1 + \lambda_2 v_2 + \lambda_3 v_3.$$

2) Dacă $\alpha_1 v_1 + \alpha_2 v_2 + \alpha_3 v_3 = 0$, cu $\alpha_1, \alpha_2, \alpha_3 \in \mathbf{R}$, atunci $\alpha_1 = \alpha_2 = \alpha_3 = 0$.

În adevăr, fie $x \in \mathbf{R}^3$, $x = (a_1, a_2, a_3)$. Pentru a arăta că 1) este adevărat trebuie să determinăm $\lambda_1, \lambda_2, \lambda_3 \in \mathbf{R}$ astfel încît

$$x = \lambda_1 v_1 + \lambda_2 v_2 + \lambda_3 v_3.$$

Avem :

$$(a_1, a_2, a_3) = x = \lambda_1 v_1 + \lambda_2 v_2 + \lambda_3 v_3 = \lambda_1(1, 1, 1) + \lambda_2(0, 1, 1) + \lambda_3(0, 0, 1) = (\lambda_1, \lambda_1, \lambda_1) + (0, \lambda_2, \lambda_2) + (0, 0, \lambda_3) = (\lambda_1, \lambda_1 + \lambda_2, \lambda_1 + \lambda_2 + \lambda_3)$$

de unde

$$\begin{cases} \lambda_1 = a_1, \\ \lambda_1 + \lambda_2 = a_2, \\ \lambda_1 + \lambda_2 + \lambda_3 = a_3. \end{cases}$$

Rezultă că $\lambda_1 = a_1$, $\lambda_2 = a_2 - a_1$, $\lambda_3 = a_3 - a_2$ și 1) este verificat. Fie acum $\alpha_1, \alpha_2, \alpha_3 \in \mathbf{R}$ astfel încît

$$\alpha_1 v_1 + \alpha_2 v_2 + \alpha_3 v_3 = 0.$$

Deducem că

$$(\alpha_1, \alpha_1 + \alpha_2, \alpha_1 + \alpha_2 + \alpha_3) = (0, 0, 0),$$

deci

$$\begin{cases} \alpha_1 = 0, \\ \alpha_1 + \alpha_2 = 0 \\ \alpha_1 + \alpha_2 + \alpha_3 = 0, \end{cases}$$

de unde $\alpha_1 = \alpha_2 = \alpha_3 = 0$.

Exemple ca cele de mai sus justifică introducerea următorului concept :

3.1. *Definiție.* **Fie V un spațiu vectorial peste corpul K. Un sistem $\mathbf{B} = (e_1, e_2, \dots, e_n)$ de vectori $e_i \in V$, $1 \leqslant i \leqslant n$, se numește** ***bază*** **a lui V dacă :**

1) $\forall x \in V$, $\exists \lambda_1, \lambda_2, \dots, \lambda_n \in K$ astfel încît

$$x = \lambda_1 e_1 + \lambda_2 e_2 + \dots + \lambda_n e_n ;$$

2) Dacă $\alpha_1 e_1 + \alpha_2 e_2 + \dots + \alpha_n e_n = 0$, cu $\alpha_1, \alpha_2, \dots, \alpha_n \in K$, atunci $\alpha_1 = \alpha_2 = \dots = \alpha_n = 0$.

Din cele de mai sus rezultă că orice sistem $\mathbf{B} = (v_1, v_2)$ format cu doi vectori diferiți de zero necoliniari formează o bază a spațiului V al vectorului de poziție dintr-un plan euclidian.

Sistemul $\mathbf{B} = (v_1, v_2, v_3)$, unde $v_1 = (1, 1, 1)$, $v_2 = (0, 1, 1)$, $v_3 = (0, 0, 1)$ formează o bază a spațiului vectorial $\mathbf{R}^3$.

2. **Dependență și independență liniară.** Strîns legate de noțiunea de bază a unui spațiu vectorial V peste un corp K sînt conceptele următoare :

i) Dacă $v_1, v_2, \dots, v_m \in V$, atunci un vector de forma

$$\lambda_1 v_1 + \lambda_2 v_2 + \dots + \lambda_m v_m \qquad (\lambda_i \in K)$$

se numește *combinație liniară* (cu coeficienți în K) de vectorii $v_1, v_2, \dots, v_m$; scalarii $\lambda_1, \lambda_2, \dots, \lambda_m$ se numesc *coeficienții* combinației liniare.

ii) Spunem că un vector $x \in V$ este *combinație liniară* (cu coeficienți în K) de vectorii $v_1, v_2, \dots, v_m$ dacă există $\lambda_1, \lambda_2, \dots, \lambda_m \in K$ astfel încît

$$x = \lambda_1 v_1 + \lambda_2 v_2 + \dots + \lambda_m v_m = \sum_{i=1}^{m} \lambda_i v_i.$$

Spunem că vectorii $v_1, v_2, \dots, v_m$ formează un *sistem de generatori* pentru spațiul vectorial V dacă orice vector $x \in V$ se poate reprezenta ca o combinație liniară de $v_1, v_2, \dots, v_m$:

$$\forall x \in V, \ \exists \lambda_1, \lambda_2, \dots, \lambda_m \in K \text{ astfel încît } x = \sum_{i=1}^{m} \lambda_i v_i.$$

iii) Spunem că sistemul de vectori $v_1, v_2, \dots, v_m$ este *liniar independent* (peste K) dacă

$$\alpha_1 v_1 + \alpha_2 v_2 + \dots + \alpha_m v_m = 0 \Rightarrow \alpha_1 = \alpha_2 = \dots = \alpha_m = 0.$$

În caz contrar spunem că vectorii $v_1, v_2, \dots, v_m$ sînt *liniar dependenți* (peste K). Așadar, vectorii $v_1, v_2, \dots, v_m$ sînt liniar dependenți (peste K) dacă există $\alpha_1, \alpha_2, \dots, \alpha_m \in K$, *nu toți nuli*, astfel încît

$$\alpha_1 v_1 + \alpha_2 v_2 + \dots + \alpha_m v_m = 0.$$

O egalitate de forma :

$$\alpha_1 v_1 + \alpha_2 v_2 + \dots + \alpha_m v_m = 0, \qquad (\alpha_i \in K)$$

se numește *relație de dependență liniară* a vectorilor $v_1, v_2, \dots, v_m$; dacă cel puțin unul dintre scalarii $\alpha_1, \alpha_2, \dots, \alpha_m$ este diferit de zero spunem că avem o relație de dependență liniar *nebanală*.

Așadar, vectorii $v_1, v_2, \ldots, v_n$ sînt liniar independenți dacă și numai dacă singura relație de dependență liniară a lor este cea banală. De asemenea, un sistem de vectori $\mathbf{B}$ este bază a lui V dacă și numai dacă $\mathbf{B}$ este sistem de generatori liniar independent.

Fie $\mathbf{B} = (e_1, e_2, \ldots, e_n)$ o bază a spațiului vectorial V peste corpul K. Dacă $x \in V$, atunci există $\lambda_1, \lambda_2, \ldots, \lambda_n \in K$ astfel încît

$$x = \lambda_1 e_1 + \lambda_2 e_2 + \ldots + \lambda_n e_n = \sum_{i=1}^{m} \lambda_i e_i.$$

Să observăm că scalarii $\lambda_1, \lambda_2, \ldots, \lambda_n$ sînt unic determinați de vectorul x și baza $\mathbf{B}$. În adevăr, dacă pentru $\lambda_1', \lambda_2', \ldots, \lambda_n' \in K$ avem de asemenea

$$x = \lambda_1' e_1 + \lambda_2' e_2 + \ldots + \lambda_n' e_n = \sum_{i=1}^{n} \lambda_i' e_i,$$

atunci

$$(\lambda_1 - \lambda_1')e_1 + (\lambda_2 - \lambda_2')e_2 + \ldots + (\lambda_n - \lambda_n')e_n = \sum_{i=1}^{n} \lambda_i e_i - \sum_{i=1}^{n} \lambda_i' e_i = x - x = 0$$

și cum sistemul de vectori $e_1, e_2, \ldots, e_n$ este liniar independent, rezultă că

$$\lambda_1 - \lambda_1' = \lambda_2 - \lambda_2' = \ldots = \lambda_n - \lambda_n' = 0,$$

deci

$$\lambda_i = \lambda_i', \quad 1 \leqslant i \leqslant n.$$

4.2. *Definiție.* **Fie V un spațiu vectorial peste corpul K, $\mathbf{B} = (e_1, e_2, \ldots, e_n)$ o bază a lui V și x un vector din V. Scalarii unic determinați $\lambda_1, \lambda_2, \ldots, \lambda_n \in K$ astfel încît**

$$x = \lambda_1 e_1 + \lambda_2 e_2 + \ldots + \lambda_n e_n$$

se numesc *coordonatele* vectorului x în baza $\mathbf{B}$.

Exemplu

Coordonatele în baza canonică a lui $\mathbf{R}^n$. În spațiul vectorial $\mathbf{R}^3$ să considerăm vectorii $e_1 = (1, 0, 0)$, $e_2 = (0, 1, 0)$, $e_3 = (0, 0, 1)$.

Dacă $x \in \mathbf{R}^3$, $x = (a_1, a_2, a_3)$, atunci:

$$x = (a_1, 0, 0) + (0, a_2, 0) + (0, 0, a_3) = a_1(1, 0, 0) + a_2(0, 1, 0) + a_3(0, 0, 1) = a_1 e_1 + a_2 e_2 + a_3 e_3,$$

deci $\mathbf{B} = (e_1, e_2, e_3)$ este un sistem de generatori pentru $\mathbf{R}^3$.

Dacă pentru $\alpha_1, \alpha_2, \alpha_3 \in \mathbf{R}$ avem

$$\alpha_1 e_1 + \alpha_2 e_2 + \alpha_3 e_3 = 0,$$

atunci

$$(\alpha_1, \alpha_2, \alpha_3) = (0, 0, 0),$$

de unde $\alpha_1 = \alpha_2 = \alpha_3 = 0$. Aşadar sistemul de vectori **B** este şi liniar independent, deci bază a spaţiului vectorial $\mathbf{R}^3$, numită *baza canonică* a lui $\mathbf{R}^3$. Cum pentru orice $x \in \mathbf{R}^3$, $x = (a_1, a_2, a_3)$ avem

$$x = a_1e_1 + a_2e_2 + a_3e_3,$$

rezultă că coordonatele în baza canonică ale unui vector $x \in \mathbf{R}^3$ coincid cu componentele acestuia.

Să observăm că coordonatele unui vector diferă de la o bază la alta. Astfel, dacă $v = (3, -2, 5) \in \mathbf{R}^3$, cum

$$v = 3e_1 - 2e_2 + 5e_3$$

coordonatele lui v în baza canonică a lui $\mathbf{R}^3$ sînt 3, —2, 5 (egale cu componentele lui v). Pe de altă parte, vectorii $v_1 = (-1, 1, 1)$, $v_2 = (1, -1, 1)$, $v_3 = (1, 1, -1)$, formează, de asemenea, o bază a lui $\mathbf{R}^3$ (v. Ex. R—1) şi coordonatele lui $v = (3, -2, 5)$ în baza v_1, v_2, v_3 sînt $\frac{3}{2}$, 4, $\frac{1}{2}$ pentru că

$$v = \frac{3}{2}v_1 + 4v_2 + \frac{1}{2}v_3.$$

Analog, în spaţiul vectorial $\mathbf{R}^n$ (sau chiar în K^n, K corp oarecare) vectorii
$e_1 = (1, 0, \ldots, 0)$, $e_2 = (0, 1, \ldots, 0)$, $\ldots$, $e_n = (0, 0, \ldots, 1)$ formează o bază a lui $\mathbf{R}^n$ (resp. K^n) numită *baza canonică* a lui $\mathbf{R}^n$ (resp. K^n). Mai mult pentru orice $x = (a_1, a_2, \ldots, a_n)$ avem

$$x = a_1e_1 + a_2e_2 + \ldots + a_ne_n,$$

deci coordonatele lui x în baza canonică coincid cu componentele sale, anume $a_1, a_2, \ldots, a_n$.

Exerciţiu rezolvat

R — 1 În spaţiul vectorial $\mathbf{R}^3$ considerăm vectorii $v_1 = (a, 1, 1)$, $v_2 = (1, a, 1)$, $v_3 = (1, 1, a)$, unde a este parametru real.

1) Arătaţi că sistemul de vectori v_1, v_2, v_3 este liniar dependent dacă şi numai dacă $a = 1$ sau $a = -2$.

2) Dacă $a \neq 1$ şi $a \neq -2$, atunci $\mathbf{B} = (v_1, v_2, v_3)$ este bază a lui V. Cînd $a = -1$, găsiţi coordonatele vectorului $v = (3, 2, 5)$ în baza B.

Soluţie. 1) Fie $\alpha_1, \alpha_2, \alpha_3 \in \mathbf{R}$ astfel încît

$$\alpha_1v_1 + \alpha_2v_2 + \alpha_3v_3 = 0.$$

Atunci

$$(a\alpha_1 + \alpha_2 + \alpha_3 ; \alpha_1 + a\alpha_2 + \alpha_3 ; \alpha_1 + \alpha_2 + a\alpha_3) = (0, 0, 0),$$

ceea ce este echivalent cu :

$$(S_0)\begin{cases} a\alpha_1 + \alpha_1 + \alpha_3 = 0, \\ \alpha_1 + a\alpha_2 + \alpha_3 = 0, \\ \alpha_1 + \alpha_2 + a\alpha_3 = 0. \end{cases}$$

Sistemul omogen (S_0) în necunoscutele $\alpha_1, \alpha_2, \alpha_3$ admite soluţii nebanale dacă şi numai dacă

$$\Delta = \begin{vmatrix} a & 1 & 1 \\ 1 & a & 1 \\ 1 & 1 & a \end{vmatrix} = 0$$

deci dacă şi numai dacă $(a + 2)(a - 1)^2 = 0$. Rezultă că vectorii v_1, v_2, v_3 sînt liniar dependenţi dacă şi numai dacă $a = -2$ sau $a = 1$.

2) Fie $x \in \mathbf{R}^3$, $x = (a_1, a_2, a_3)$. Să arătăm că se pot determina scalarii $\lambda_1, \lambda_2, \lambda_3 \in \mathbf{R}$ astfel încît

$$x = \lambda_1 v_1 + \lambda_2 v_2 + \lambda_3 v_3.$$

Trebuie să avem

$$(a\lambda_1 + \lambda_2 + \lambda_3, \lambda_1 + a\lambda_2 + \lambda_3, \lambda_1 + \lambda_2 + a\lambda_3) = (a_1, a_2, a_3)$$

ceea ce este echivalent cu :

$$(S)\begin{cases} a\lambda_1 + \lambda_2 + \lambda_3 = a_1, \\ \lambda_1 + a\lambda_2 + \lambda_3 = a_2, \\ \lambda_1 + \lambda_2 + a\lambda_3 = a_3. \end{cases}$$

Cum $a \neq 1$ şi $a \neq -2$ determinantul Δ al sistemului (S) este diferit de zero.

$$\Delta = (a + 2)(a - 1)^2 \neq 0.$$

În acest caz sistemul (S) admite soluţie (chiar unică). Conform regulii lui Cramer aceasta este

$$\lambda_1 = \frac{a^2 - 1}{\Delta} a_1 + \frac{1 - a}{\Delta} a_2 + \frac{1 - a}{\Delta} a_3,$$

$$\lambda_2 = \frac{1 - a}{\Delta} a_1 + \frac{a^2 - 1}{\Delta} a_2 + \frac{1 - a}{\Delta} a_3,$$

$$\lambda_3 = \frac{1 - a}{\Delta} a_1 + \frac{1 - a}{\Delta} a_2 + \frac{a^2 - 1}{\Delta} a_3.$$

Cînd $a = -1$ şi $a_1 = 3$, $a_2 = -2$, $a_3 = 5$ avem $\Delta = 4$ şi aplicînd formulele de mai sus găsim $\lambda_1 = 3/2$, $\lambda_2 = 4$, $\lambda_3 = 1/2$, deci

$$v = (3, -2, 5) = \frac{3}{2} v_1 + 4v_2 + \frac{1}{2} v_3.$$

Exerciţii

1. Verificaţi proprietăţile S_1, S_2 şi S_4 pentru înmulţirea matricelor cu scalari.
2. Verificaţi proprietăţile S_2, S_3 şi S_4 pentru înmulţirea polinoamelor cu scalari.
3. Fie M o mulţime nevidă şi $\mathcal{F}(M)$ mulţimea tuturor funcţiilor $f: M \to M$. Pe M definim legea de compoziţie externă cu operatori în $\mathcal{F}(M)$.

$$\mathcal{F}(M) \times M \to M, \ (f, x) \to f * x \overset{\text{def}}{=} f(x) \in M.$$

Arătaţi că :

1) $f*(g*x) = (f*g)*x, \quad \forall f, g \in \mathcal{F}(M), \quad x \in M$;

1) $1_M*x = x, \quad \forall x \in M$.

4. Fie $V = \mathbf{R}_+^* = \{x \in \mathbf{R} \mid x > 0\}$. Arătaţi că V este spaţiu vectorial peste corpul $\mathbf{R}$ în raport cu legile de compoziţie.

$$x \perp y \overset{\text{def}}{=} xy, \qquad \alpha \top x \overset{\text{def}}{=} x^\alpha, \qquad \forall \alpha \in \mathbf{R},\ x \in V.$$

5. Fie V mulţimea tuturor şirurilor f de numere reale,

$$f = (a_0, a_1, \ldots, a_n, \ldots,)\ (a_i \in \mathbf{R}).$$

Dacă $\alpha \in \mathbf{R}$ şi $f, g \in V$, $f = (a_0, a_1, \ldots, a_n, \ldots)$, $g = (b_0, b_1, \ldots, b_n, \ldots)$ atunci punem

$$f + g \overset{\text{def}}{=} (a_0 + b_0, a_1 + b_1, \ldots, a_n + b_n, \ldots)$$

$$\alpha f \overset{\text{def}}{=} (\alpha a_0, \alpha a_1, \ldots, \alpha a_n, \ldots).$$

Arătaţi că V este spaţiu vectorial peste corpul $\mathbf{R}$ în raport cu legile de compoziţie :

$$V \times V \to V, \qquad (f, g) \to f + g$$

$$\mathbf{R} \times V \to V, \qquad (\alpha, f) \to \alpha f.$$

6. Fie $K = \mathbf{Z}_2 = \{\hat{0}, \hat{1}\}$. Enumeraţi toţi vectorii spaţiului vectorial K^3. Care este numărul vectorilor spaţiului vectorial K^n ?

7. Arătaţi că pentru oricare două numere naturale p, n, cu p prim, există un spaţiu vectorial V cu p^n vectori.

8. Fie $V \neq 0$ un spaţiu vectorial peste corpul $\mathbf{R}$. Arătaţi că E are o infinitate de vectori.

9. Fie V un spaţiu vectorial peste corpul Z_p, p număr prim. Arătaţi că

$$0 = x + x + \ldots + x (p \text{ ori}), \qquad \forall x \in V.$$

10. Fie V un spaţiu vectorial peste corpul K. Demonstraţi prin inducţie că

$$\alpha(v_1 + v_2 + \ldots + v_n) = \alpha v_1 + \alpha v_2 + \ldots + \alpha v_n$$

şi

$$(\alpha_1 + \alpha_2 + \ldots + \alpha_m)v = \alpha_1 v + \alpha_2 v + \ldots + \alpha_m v$$

oricare ar fi $\alpha, \alpha_1, \ldots, \alpha_m \in K$, $v, v_1, \ldots, v_n \in V$.

11. Fie vectorii $v_1 = (1, 1, 0)$, $v_2 = (0, 1, 1)$, $v_3 = (1, 0, 1)$ din spaţiul vectorial $\mathbf{R}^3$.

1) Arătaţi că sistemul de vectori $\mathbf{B} = (v_1, v_2, v_3)$ este o bază a lui $\mathbf{R}^3$.

2) Reprezentaţi vectorul $v = (2, -3, 5)$ ca o combinaţie liniară de vectorii bazei $\mathbf{B}$.

12. În spaţiul vectorial $V = M_2(\mathbf{R})$ se consideră matricele

$$E_1 = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \quad E_2 = \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}, \quad E_3 = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, \quad E_4 = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}, \quad A = \begin{pmatrix} -2 & 3 \\ 4 & -2 \end{pmatrix}.$$

1) Arătaţi că $\mathbf{B} = (E_1, E_2, E_3, E_4)$ este o bază a lui V.

2) Reprezentaţi matricea A ca o combinaţie liniară de vectorii bazei $\mathbf{B}$.

13. Fie $f_1, f_2, f_3 \in \mathbf{R}[X]$, $f_1 = (X-b)(X-c)$, $f_2 = (X-c)(X-a)$, $f_3 = (X-a)(X-b)$.

1) Arătaţi că polinoamele f_1, f_2, f_3 sînt liniar independente peste $\mathbf{R}$ dacă şi numai dacă $(a-b)(b-c)(c-a) \neq 0$.

2) Arătaţi că pentru orice polinom $f \in \mathbf{R}[X]$ cu grad $f \leqslant 2$, există $\lambda_1, \lambda_2, \lambda_3 \in \mathbf{R}$ unic determinaţi astfel încît

$$f = \lambda_1 f_1 + \lambda_2 f_2 + \lambda_3 f_3.$$

3) Determinaţi $\lambda_1, \lambda_2, \lambda_3$ cînd $f = 1 + 2X - X^2$, $a = 1$, $b = 2$, $c = 3$.

14. Arătaţi că fiecare din sistemele de polinoame din $\mathbf{R}[X]$,

$$\mathbf{B} = (1, X, X^2, X^3),$$

$$\mathbf{B}' = (1 + X^2, X + X^2, X^2, X^3 + X^2)$$

$$\mathbf{B}'' = (1, X - 1, (X - 1)^2/2\,!, (X - 1)^3/3\,!)$$

sînt liniar independente peste $\mathbf{R}$ şi reprezentaţi polinomul $f = X^3 - X^2 - X + 1$ ca o combinaţie liniară cu coeficienţi din $\mathbf{R}$ de polinoamele din $\mathbf{B}$ (resp. $\mathbf{B}'$, $\mathbf{B}''$).

15. Fie V un spaţiu vectorial peste corpul K şi v_1, v_2, v_3 un sistem de vectori liniar independenţi. Arătaţi că vectorii $v_1 + v_2$, $v_2 + v_3$, $v_3 + v_1$, sînt, de asemenea, liniar independenţi.

16. Fie v_1, v_2, v_3 un sistem de vectori dintr-un spaţiu vectorial V peste corpul K. Arătaţi că aplicaţia

$$f : K^3 \to V,\ f(x) = \lambda_1 v_1 + \lambda_2 v_2 + \lambda_3 v_3\ \forall x = (\lambda_1, \lambda_2, \lambda_3) \in \mathbf{R}$$

este injectivă (surjectivă, bijectivă) dacă şi numai dacă v_1, v_2, v_3 este un sistem liniar independent (resp. sistem de generatori ai lui V, bază a lui V). Generalizare.

INDICAŢII ŞI RĂSPUNSURI

CAPITOLUL I

3. 1) Pentru orice $x \in \mathbf{R}$ avem $(f_{a,b} \circ f_{c,d}(x)) = f_{a,b}(f_{c,d}(x)) = acx + ad + b = f_{ac,\,ad+b}(x)$; 2) $\alpha = a^{-1}$, $\beta = a^{-1}b$.

4. Pentru orice $x \in \mathbf{Z} \times \mathbf{Z}$, $f_A(x)$ are a 2-a componentă pară, deci f_A nu este surjectivă ; pentru orice $y \in \mathbf{Q} \times \mathbf{Q}$, $y = (y_1, y_2)$, sistemul de ecuaţii $3x_1 + x_2 = y_1$, $4x_1 + 2x_2 = y_2$ are soluţie unică, deci f_A este bijectivă.

6. Primele egalităţi prin verificare directă. Apoi se poate continua astfel :

$$R_\theta S_{\theta'} = R_\theta R_{\theta'} \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = R_{\theta+\theta'} \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = S_{\theta+\theta'} \text{ etc.}$$

7. Puneţi condiţia ca A să comute cu matricele $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$, $\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$ şi se obţine că 2) $\Rightarrow$ 1).

8. $A = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ şi $A = \begin{pmatrix} -1 & 0 \\ 1 & -1 \end{pmatrix}$.

12. Inducţie după n (v. Teorema 4.2).

13. Avem $n^5 - n = (n - 1)n(n + 1)\cdot(n^2 + 1)$ şi $240 = 2^4 \times 3 \times 5$ şi se arată că $n^5 - n$ se divide prin 2^4, 3 şi 5.

16. Se aplică regula lui Cramer.

17. Fie $e_1 = (1, 0)$, $e_2 = (0, 1)$. Cum $f_A(e_1) = f_B(e_1)$ rezultă că $(a_{11}, a_{21}) = (b_{11}, b_{21})$ iar din $f_A(e_2) = f_B(e_2)$ rezultă $(a_{12}, a_{22}) = (b_{12}, b_{22})$, deci $A = B$ etc.

18. Dacă $A^2 = -E$, atunci $A = \begin{pmatrix} a & b \\ c & -a \end{pmatrix}$ cu $a, b, c \in \mathbf{Z}$, $a^2 + bc + 1 = 0$. De exemplu $A = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 3 & 5 \\ -2 & -3 \end{pmatrix}$.

19. Fie $A = \begin{pmatrix} a & c \\ b & d \end{pmatrix}$. Atunci $A^T = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ și din $A^T A = E$ rezultă :

$$1 = \det(E) = \det(A^T)\det(A) = (ad - bc)^2,$$

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = E = A^T A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} a & c \\ b & d \end{pmatrix} = \begin{pmatrix} a^2 + b^2 & ac + bd \\ ca + db & c^2 + d^2 \end{pmatrix},$$

deci $ad - bc = \pm 1$, $a^2 + b^2 = 1$, $ac + bd = 0$, $c^2 + d^2 = 1$. Dacă $ad - bc = 1$, atunci $c = -b$, $a = d$. Cum $a^2 + b^2 = 1$, există $\theta \in [0, 2\pi)$ astfel încît $a = \cos\theta$ și $b = \sin\theta$ etc.

20. 4) $B = \frac{1}{2}(A + A^T)$, $C = \frac{1}{2}(A - A^T)$.

21. Există n astfel încît $a = bq_0 + r_0$, $b = r_0 q_1 + r_1$, $r_0 = r_1 q_2 + r_2$, $\ldots$, $r_{n-2} = r_{n-1}q_n + r_n$, $r_{n-1} = r_n q_{n+1} + 0$, cu $0 < r_n < r_{n-1} < \ldots < r_0 < b$ (algoritmul lui Euclid pentru a și b). Atunci :

$$r_n = (r_n, 0) = (r_{n-1}, r_n) = (r_{n-2}, r_{n-1}) = \ldots = (r_0, r_1) = (b, r_0) = (a, b).$$

22. Fie $q, r \in \mathbf{N}$ astfel încît $a = bq + r$, $0 \leqslant r < b$. Avem :

$$2^a - 1 = 2^{bq+r} - 1 = (2^{bq} - 1)2^r + 2^r - 1 = (2^b - 1)Q + 2^r - 1, \text{ unde}$$

$Q = (2^{b(q-1)} + 2^{b(q-2)} + \ldots + 2^b + 1)$ și $2^r - 1 < 2^b - 1$. Deci dacă r este restul împărțirii lui a prin b, atunci $2^r - 1$ este restul împărțirii lui $2^a - 1$ prin $2^b - 1$. În particular, dacă d este ultimul rest diferit de zero din algoritmul lui Euclid pentru a și b, atunci $2^d - 1$ este ultimul rest diferit de zero din algoritmul lui Euclid pentru $2^a - 1$ și $2^b - 1$, de unde $(2^a - 1, 2^b - 1) = 2^{(a, b)} - 1$.

23. Conform Ex. 22 este suficient să arătăm că numerele $6q - 1$, $6q + 1$, $6q + 2$, $6q + 3$, $6q + 5$, $6q + 7$ sînt relativ prime în perechi. Dacă un număr prim p divide două din ele, atunci divide și diferența lor în valoare absolută. Diferențele în valoare absolută posibile sînt 2, 3, 4, 6, 8, 1, 5, deci p poate fi 2, 3 sau 5. Se observă că 2 divide doar pe $6q + 2$ iar 3 doar pe $6q + 3$. Singura complicație poate apărea cînd 5 divide pe $6q + 2$ și $6q + 7$, ceea ce se exclude prin ipoteza $q \not\equiv 3 \pmod 5$.

CAPITOLUL II

1. Vezi Tablele II-1 și II-2.

2. Vezi Tabla II-3.

3. Vezi Tablele II-4 și II-5.

4. Vezi Tablele II-6 și II-7.

5. Dacă $x, y \in (2, \infty)$ atunci $x - 2 > 0$, $y - 2 > 0$, deci $xy - 2(x + y) + 4 = (x - 2)(y - 2) > 0$. Cum $x * y = xy - 2(x + y) + 4 + \lambda - 4$, trebuie ca $\lambda \geqslant 6$.

6. Vezi Tabla II-8.

$\oplus$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

Tabla II-1

$\otimes$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

Tabla II-2

	0	1	2	3	4
0	0	1	2	3	4
1	1	0	1	2	3
2	2	1	0	1	2
3	3	2	1	0	1
4	4	3	2	1	0

Tabla II-3

$\perp$	α	β	γ
α	α	α	α
β	α	β	γ
γ	α	γ	γ

Tabla II-4

$\top$	α	β	γ
α	α	β	γ
β	β	β	β
γ	γ	β	γ

Tabla II-5

$\circ$	f_1	f_2	f_3
f_1	f_1	f_2	f_3
f_2	f_2	f_3	f_1
f_3	f_3	f_1	f_2

Tabla II-8

$\perp$	1	2	3	4	6	12
1	1	1	1	1	1	1
2	1	2	1	2	2	2
3	1	1	3	1	3	3
4	1	2	1	4	2	4
6	1	2	3	2	6	6
12	1	2	3	4	6	12

Tabla II-6

$\top$	1	2	3	4	6	12
1	1	2	3	4	6	12
2	2	2	6	4	6	12
3	3	6	3	12	6	12
4	4	4	12	4	12	12
6	6	6	6	12	6	12
12	12	12	12	12	12	12

Tabla II-7

7. Elementul neutru este 0. Dacă, $x, y \in [-1, \infty)$ atunci $x + 1 \geqslant 0$, $y + 1 \geqslant 0$, deci $x + y + xy + 1 = (y + 1)(x + 1) \geqslant 0$, de unde $x * y \in [-1, \infty)$.

8. Operația „$\perp$" admite ca element neutru pe b cînd H este $[a, b]$ sau $(a, b]$ iar operația „$\top$" admite ca element neutru pe a cînd H este $[a, b]$ sau $[a, b)$.

9. Operația „$\top$" admite ca element neutru pe 1. Operația „$\perp$" nu admite element neutru, iar cea indusă pe H de „$\perp$" admite ca element neutru pe 12.

12. Dacă $e \in \mathbf{Z}$ este element neutru, puneți condițiile $e*0 = 0$ și $e*1 = 1$.

13. $(1, n, p)$, $(m, n, 1)$, $(m, 2, 2)$;

14. $a = 0$, $b = 0$, sau $a = \dfrac{1}{2}$, $b = 1$.

15. $e = 2$.

16. 3) Avem $AV = A$, $\forall A \in M$ dacă $V = \begin{pmatrix} 0 & c \\ 0 & 1 \end{pmatrix}$ cu $c \in \mathbf{R}$.

18. Operația „$*$" nu este asociativă și admite element neutru matricea $\dfrac{1}{2}E$, unde E este matricea unitate.

20. Fie $x, y \in H$, $x = a + b\sqrt{2}$, $y = c + d\sqrt{2}$, atunci $xy = (ac + 2bd) + (ad + bc)\sqrt{2}$ și $(ac + 2bd)^2 - 2(ad + bc)^2 = a^2(c^2 - 2d^2) - 2b^2(c^2 - 2d^2) = 1$, deci $xy \in H$. Cum $(a + b\sqrt{2})(a - b\sqrt{2}) = a^2 - 2b^2 = 1$, avem $x^{-1} = a - b\sqrt{2}$.

21. 2) A este simetrizabil dacă și numai dacă $a \neq 0$ și $b \neq 0$ și avem

$$A^{-1} = \begin{pmatrix} a^{-1} & 0 \\ -ca^{-1}b^{-1} & b^{-1} \end{pmatrix}.$$

24. $x = 1,\ y = 2$.

25. Elementul neutru este $(1, 0)$, elementele simetrizabile sînt $(1, b)$ şi $(-1, b)$ cu $b \in \mathbf{Z}$.

26. Fie $b \in M$ astfel încît $a = aba$. Fie $e = ab$ şi $f = ba$. Avem $ey = abaxa = axa = y$ şi $yf = axaba = axa = y$, $\forall y \in M$. În particular $e = ef = f$.

27. Luînd x arbitrar, $y = e$, $u = e$ şi $v = e'$ se obţine $x = x \perp e$. Luînd $x = e'$, $y = e'$, $u = e$ şi v arbitrar se obţine $v = e \perp v$, de unde $e = e'$. Acum avem $x \perp y = (x \top e) \perp \perp (e \top y) = (x \perp e) \top (e \perp y) = x \top y$, $\forall x, y \in M$. De asemenea, $x \perp y = (e \top x) \perp \perp (y \perp e) = (e \perp y) \top (x \perp e) = y \top x = y \perp x$.

28. 1) 3^9 ; 2) 3^6 ; 3) 3^5. În general, pentru o mulţime cu n elemente, avem : n^{n^2}, $n^{n(n+1)^2}$, $n^{(n-1)^2+1}$ respectiv.

30. Orice cuvînt $\alpha \in M$ se poate scrie sub formă $\alpha = \alpha'\alpha''$, unde α' este secvenţa formată cu primele 5 litere ale lui α ; α'' este secvenţa formată cu următoarele 3 litere ale lui α. Dacă $\alpha, \beta, \gamma \in M$, $\alpha = \alpha'\alpha''$, $\beta = \beta'\beta''$, $\gamma = \gamma'\gamma''$, atunci $(\alpha * \beta) * \gamma = (\alpha'\beta'') * (\gamma'\gamma'') = \alpha'\gamma'' = (\alpha'\alpha'') * (\beta'\gamma'') = \alpha * (\beta * \gamma)$.

CAPITOLUL III

1. ± 1, $\pm i$.

2. Dacă $x, y \in (-1, 1)$, atunci $(x + y)/(x + xy) \in (-1, 1)$. Elementul neutru este 0 iar simetricul lui x este $-x$.

3. Vezi tabla III-1. **4.** Vezi Tabla III-2. **5.** Vezi Tabla III-3.

$\cdot$	1	ε	ε^2
1	1	ε	ε^2
ε	ε	ε^2	1
ε^2	ε^2	1	ε

Tabla III-1

$\circ$	f_1	f_2	f_3	f_4
f_1	f_1	f_2	f_3	f_4
f_2	f_2	f_1	f_4	f_3
f_3	f_3	f_4	f_1	f_2
f_4	f_4	f_3	f_2	f_1

Tabla III-2

$\circ$	f_1	f_2	f_3	f_4	f_5	f_6
f_1	f_1	f_2	f_3	f_4	f_5	f_6
f_2	f_2	f_3	f_1	f_6	f_4	f_5
f_3	f_3	f_1	f_2	f_5	f_6	f_4
f_4	f_4	f_5	f_6	f_1	f_2	f_3
f_5	f_5	f_6	f_4	f_3	f_1	f_2
f_6	f_6	f_4	f_5	f_2	f_3	f_1

Tabla III-3

10. Avem $xyxy = xxyy$. Înmulţind la stînga cu x^{-1} şi la dreapta cu y^{-1}, rezultă $xy = yx$.

11. Avem $(xy)^2 = e = ee = x^2y^2$ şi se aplică Ex. 10.

12. Pentru x arbitrar şi $y = e$ rezultă $x = (x \top x) \top x$. Deci $x \top x = e$, de unde $x \perp y = x \top y$. Aplicînd Ex. 11, deducem şi $x \perp y = y \perp x$.

13. $\xi = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$. **14.** $x = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 2 & 1 \end{pmatrix}$, $y = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 2 & 4 \end{pmatrix}$.

15. Cînd $h \geq 0$ şi $k \geq 0$ demonstraţie prin inducţie. Dacă $h < 0$ şi $k < 0$, atunci $a^h b^k = (a^{-h})^{-1}(b^{-k})^{-1} = (b^{-k}a^{-h})^{-1} = (a^{-h}b^{-k})^{-1} = (b^{-k})^{-1}(a^{-h})^{-1} = b^k a^h$ etc.

16. Din $ab = b^4a$ rezultă că $b^4 = aba^{-1}$. Atunci $b^2 = b^2b^6 = b^4b^4 = aba^{-1}aba^{-1} = ab^2a^{-1}$, de unde $b^2a = ab^2$. Atunci $ab^3 = b^2ab = b^2b^4a = a$, de unde $b^3 = e$. Înmulţind la stînga şi dreapta cu b egalitatea $b^2a = ab^2$ rezultă $ab = ba$.

17. Vezi Teoremele 4.1 şi 4.2, Cap. III, § 4.

19. Evident $12\mathbf{Z} \subseteq 3\mathbf{Z} \cap 4\mathbf{Z}$. Dacă $a \in 3\mathbf{Z} \cap 4\mathbf{Z}$, atunci $3 \mid a$ și $4 \mid a$ și cum $(3, 4) = 1$ rezultă că $3 \times 4 = 12$ divide a, deci $a \in 12\mathbf{Z}$.

20. a) $H = (\mathbf{Z}, +)$; b) $H = (\mathbf{Q}, +)$.

24. Se observă că $f(x) \in (-1, 1)$, $\forall x \in (0, \infty)$ și $f(xy) = f(x) * f(y)$.

25. Funcția $f : G \to \mathbf{R}$, $f(x) = \text{tg}(x)$, $\forall x \in G$ este un izomorfism de la $(G, *)$ la $(\mathbf{R}, +)$.

26. 1) Vezi Tabla III-4. 2) Definiți $f : \mathcal{K} \to G$ prin $f(e) = E$, $f(u) = A$, $f(v) = B$ și $f(w) = E$.

$\cdot$	E	A	B	C
E	E	A	B	C
A	A	E	C	B
B	B	C	E	A
C	C	B	A	E

Tabla III-4

Δ	$\varnothing$	$\{a\}$	$\{b\}$	$\{a, b\}$
$\varnothing$	$\varnothing$	$\{a\}$	$\{b\}$	$\{a, b\}$
$\{a\}$	$\{a\}$	$\varnothing$	$\{a, b\}$	$\{b\}$
$\{b\}$	$\{b\}$	$\{a, b\}$	$\varnothing$	$\{a\}$
$\{a, b\}$	$\{a, b\}$	$\{b\}$	$\{a\}$	$\varnothing$

Tabla III-5

28. Vezi Tabla III-5 ; 2) $f(e) = \varnothing$, $f(u) = \{a\}$, $f(v) = \{b\}$, $f(w) = \{a, b\}$.

31. 1) $\Rightarrow$ 2). Fie $a \in H$. Cum H este mulțime finită, aplicația $f : H \to H$, $f(x) = ax$, este bijectivă. Există deci $b \in H$ astfel încît $ab = a$. Atunci $b = e$, deci $e \in H$. Există $a' \in H$ astfel încît $aa' = e$. Dar $a^{-1} = a' \in H$ și deci H este subgrup.

32. 2) $\Rightarrow$ 1). Există $e \in G$ astfel încît $ae = a$. Pentru $b \in G$ avem $be = yae = ya = b$. Analog există $e' \in G$ astfel încît $e'b = b$, $\forall\, b \in G$. Evident, $e = e'$. Dacă $a \in G$, există a', $a'' \in G$ astfel încît $a'a = e = aa''$ și cum $a' = a'e = a'(aa'') = (a'a)a'' = ea'' = a''$ se deduce că a^{-1} există.

33. 1) $\Rightarrow$ 2). Dacă $H = 0 = \{0\}$ se ia $n = 0$. Dacă $H \neq 0$ fie $x \in H$, $x \neq 0$. Cum și $-x \in H$ rezultă că H conține numere întregi strict pozitive și fie $n > 0$ cel mai mic număr strict pozitiv din H. Avem $n\mathbf{Z} \subseteq H$ și folosind teorema împărțirii (prin n) cu rest se arată și $H \subseteq n\mathbf{Z}$.

34. Fie $z = \cos\varphi + i\sin\varphi$. Atunci $1 = z^n = \cos n\varphi + i\sin n\varphi$ deci $n\varphi = 2k\pi$ cu $h \in \mathbf{Z}$. Rezultă că $z = \cos 2r\pi + i\sin 2r\pi$, unde $r = h/n \in \mathbf{Q}$. Reciproc, dacă $r \in \mathbf{Q}$, atunci există h, $n \in \mathbf{Z}$, $n > 0$, astfel încît $r = h/n$ și atunci $z^n = 1$ dacă $z = \cos 2r\pi + i\sin 2r\pi$.

35. Notăm elementele $1, z_1, z_2, \ldots, z_{n-1}$ ale lui H astfel încît argumentele lor să satisfacă $0 < \varphi_1 < \varphi_2 < \ldots < \varphi_{n-1} < 2\pi$. Cum argumentul lui $z_2z_1^{-1} \in H$ este $\varphi_2 - \varphi_1 > 0$, rezultă că $\varphi_2 - \varphi_1 = \varphi_1$. Exploatînd această idee se arată că $\varphi_i = i\varphi_1$ pentru $0 < i < n$ și $n\varphi_1 = 2\pi$. Rezultă că $H = H\zeta = U_n$, unde $\zeta = \cos\dfrac{2\pi}{n} + i\sin\dfrac{2\pi}{n}$ (v. Ex. R–2, § 4. Cap. III).

36. Fie $f : \mathbf{Z} \to \mathbf{Z}$ un automorfism al grupului $(\mathbf{Z}, +)$ și fie $a = f(1)$. Atunci $f(2) = f(1 + 1) = f(1) + f(1) = a + a = 2a$, $f(-2) = -f(2) = -2a$ etc., deci $f(h) = ha$, $\forall\, h \in \mathbf{Z}$. Cum f este surjectiv, există $b \in \mathbf{Z}$ astfel încît $1 = f(b) = ba$. Deducem că $a = \pm 1$. Dacă $a = 1$, atunci $f = 1_{\mathbf{Z}}$ iar dacă $a = -1$, atunci $f = -1_{\mathbf{Z}}$.

CAPITOLUL IV

1. Elementul zero al lui A este $(0, 0)$, elementul unitate este $(1, 0)$. Dacă $(a, b)(x, y) = (0, 0)$, atunci $ax + 3by = 0$ și $bx + ay = 0$. Cînd $(a, b) \neq (0, 0)$ avem $\det\begin{pmatrix} a & 3b \\ b & a \end{pmatrix} = a^2 - 3b^2 \neq 0$, de unde $x = 0$, $y = 0$, deci A nu are divizori ai lui zero.

3. Dacă „$\perp$" și „$\top$" satisfac condițiile din enunț, atunci pentru orice $x, y \in \mathbf{Z}$ avem $x + y - a = (x - a) \perp (y - a)$ și $xy - a = (x - a) \top (y - a)$. Observînd că f este bijectiv și notînd $x - a = u$, $y - a = v$, avem $u \perp v = u + v + a$ și $u \top v = uv + au + av - a^2 - a$, $\forall\, u, v \in \mathbf{Z}$. Elementul zero este $-a$, elementul unitate este $1 - a$.

5. Elementul zero este $(0, 0)$ iar $(1, 1)$ este elementul unitate al lui A. Elementele inversabile sînt $(1, 1)$, $(1, -1)$, $(-1, 1)$ și $(-1, -1)$.

7. 1) $(1, 1), (1, -1), (2, 1), (2, -1), (4, 1), (4, -1), (5, 1), (5, -1), (7, 1), (7, -1), (8, 1), (8, -1)$.

8. Vezi Tablele IV.1 și IV.2.

+	(0, 0)	(1, 0)	(0, 1)	(1, 1)
(0, 0)	(0, 0)	(1, 0)	(0, 1)	(1, 1)
(1, 0)	(1, 0)	(0, 0)	(1, 1)	(0, 1)
(0, 1)	(0, 1)	(1, 1)	(0, 0)	(1, 0)
(1, 1)	(1, 1)	(0, 1)	(1, 0)	(0, 0)

Tabla IV. 1.

·	(0, 0)	(1, 0)	(0, 1)	(1, 1)
(0, 0)	(0, 0)	(0, 0)	(0, 0)	(0, 0)
(1, 0)	(0, 0)	(1, 0)	(0, 0)	(1, 0)
(0, 1)	(0, 0)	(0, 0)	(0, 1)	(0, 1)
(1, 1)	(0, 0)	(1, 0)	(0, 1)	(1, 1)

Tabla IV. 2.

9. $x + x = (x + x)^2 = (x + x)(x + x) = x^2 + x^2 + x^2 + x^2 = x + x + x + x$, de unde $x + x = 0$ și deci $x = -x$, $\forall\, x \in B$. De asemenea,
$x + y = (x + y)^2 = (x + y)(x + y) = x^2 + yx + xy + y^2 = x + yx + xy + y$, de unde $yx + xy = 0$, deci $yx = -xy = xy$.

10. 1) 16 ; 3) Există 6 elemente inversabile.

12. 1) $a \oplus a \oplus a \oplus a \oplus a = (1 \oplus 1 \oplus 1 \oplus 1 \oplus 1) \otimes a = 0 \otimes a = 0$.
2) Se observă că $5 \mid C_5^k$, $0 < k < 5$ și se aplică 1) și Ex. 11.

13. 1) Oricare ar fi $a, b, c \in \mathbf{R}$ cu $ac = 0$; 2) $(E - U)(E + U) = E$.

14. Vezi tabla IV.3.

15. $x = \hat{2}$, $y = \widehat{11}$.

·	$\hat{1}$	$\hat{5}$	$\hat{7}$	$\widehat{11}$
$\hat{1}$	$\hat{1}$	$\hat{5}$	$\hat{7}$	$\widehat{11}$
$\hat{5}$	$\hat{5}$	$\hat{1}$	$\widehat{11}$	$\hat{7}$
$\hat{7}$	$\hat{7}$	$\widehat{11}$	$\hat{1}$	$\hat{5}$
$\widehat{11}$	$\widehat{11}$	$\hat{5}$	$\hat{7}$	$\hat{1}$

Tabla IV. 3.

21. 2) $(1, 0), (-1, 0), (0, 1), (0, -1)$; 2) Aplicația $f: \mathbf{Z}[i] \to A$, $f(z) = (a, b)$, $\forall\, z \in \mathbf{Z}[i]$, $z = a + ib$, este izomorfism.

23. Aplicația $f: \mathbf{C} \to K$, $f(z) = (a, b)$, $\forall\, z \in \mathbf{C}$, $z = a + ib$ este izomorfism.

24. Aplicația $f: K \to \mathbf{R}$, $f(x) = \ln x$, $\forall\, x \in K$, este un izomorfism.

25. Aplicația $f: \mathbf{Q}(\sqrt{2}) \to K$, $f(z) = \begin{pmatrix} a & 2b \\ b & a \end{pmatrix}$, $\forall\, z \in \mathbf{Q}(\sqrt{2})$, $z = a + b\sqrt{2}$ este izomorfism.

26. 1) $a = b = 1$, $c = 6$; 2) $\alpha = 1$, $\beta = 2$.

27. $f + g = X^2 + \hat{4}X + \hat{4}$, $fg = X^6 + X^5 + \hat{4}X^4 + \hat{4}X^3 + \hat{2}X + \hat{3}$.

28. $fg = 0$.

29. $\hat{2}X^3 + \hat{2}X^2 + \hat{1}$, $X^3 + \hat{2}X^2 + X + \hat{1}$, $\hat{2}X^2 + \hat{2}X + \hat{1}$.

30. $\hat{0}$, $\hat{1}$, $\hat{2}$, $\hat{3}$, $\hat{4}$, $\hat{5}$.

31. Fie $f = ax + b$, $g = cX + d$. Punînd condiția $f^2 + g^2 = X^2 + 1$ rezultă $a^2 + c^2 = 1$, $b^2 + d^2 = 1$, $ab + cd = 0$. De asemenea, $(2a + b)^2 + (2c + d) = 5$, $(2a + b)(2c + d) = 2$. Deci $2a + b$ și $2c + d$ sînt rădăcinile ecuației $t^2 - 5t + 2 = 0$. Se găsește $f = \frac{4}{5}X + \frac{3}{5}$, $g = \frac{3}{5}X - \frac{4}{5}$ etc.

32. grad f este 0 dacă $\lambda = 1$; 2 dacă $\lambda = 2$; 3 dacă $\lambda \neq 2$ și $\lambda \neq 1$.

33. $f = X + 2$, $g = -X - 1$.

36. $q = \hat{4}X^2 + \hat{4}X + \hat{2}$, $r = \hat{3}X + \hat{2}$.

37. $a = 14$, $b = -3$.

38. $f = -1 + 4X - 6X^2 + 4X^3$.

39. $a = \pm i$, $b = 0$; $a = 1$, $b = \pm\sqrt{2}$; $a = -1$, $b = i\sqrt{2}$.

40. $f(3) = 196$.

41. $q = \hat{5}X^3 + \hat{3}X^2 + \hat{2}X + \hat{5}$, $r = \hat{5}$.

42. Fie $a, b \in \mathbb{Z}$, $a = 2s$, $b = 2t + 1$, astfel încît $f(a) = f(b) = 0$. Cum $a \neq b$, polinomul $(X - a)(X - b)$ divide pe f, deci există $q \in \mathbb{Z}[X]$ astfel încît $f = (X - 2s)(X - 2t - 1)q$. Se observă că pentru orice $k \in \mathbb{Z}$ unul din numerele $k - 2s$, $k - 2t - 1$ este par.

43. $X^4 + 4 = (X^2 + 2X + 2)(X^2 - 2X + 2) = (X + 1 - i)(X + 1 + i)(X - 1 + i)(X - 1 - i)$, $X^6 + 27 = (X^2 + 3)(X^2 + 3X + 3)(X^2 - 3X + 3) = (X + i\sqrt{3})(X - i\sqrt{3})(X + z)(X + \bar{z})(X - \bar{z})(X - z)$, unde $z = (3 + i\sqrt{3})/2$.

44. $f = (X + \hat{2})(X + \hat{3})(X^2 + X + \hat{1})$.

45. 1) v. Ex. 2, § 7 ; 2) $f = (X - \sqrt[3]{2})(X^2 + \sqrt[3]{2}X + \sqrt[3]{4}) = (X - \sqrt[3]{2})(X - \sqrt[3]{2}\varepsilon)(X - \sqrt[3]{2}\varepsilon^2)$, unde $\varepsilon = (-1 + i\sqrt{3})/2$.

46. Cum A este mulțime finită este suficient să arătăm că f este funcție injectivă. Dacă $f(x_1) = f(x_2)$, atunci $1 + x_1 = 1 + x_2$, de unde $x_1 = x_2$, căci $(A, +)$ este grup. Așadar $A = \{f(0), f(1), f(a), f(b)\}$, deci $f(0) + f(1) + f(a) + f(b) = 0 + 1 + a + b$, ceea ce în grupul $(A, +)$ atrage $1 + 1 + 1 + 1 = 0$. Dacă A este corp și $1 + 1 \neq 0$, atunci $0 \neq (1 + 1)^2 = 1 + 1 + 1 + 1 = 0$. Contradicție.

48. Cum $1 = (-1)^6 = -1$, avem $1 + 1 = 0$, deci $a + a = a(1 + 1) = a \cdot 0 = 0$, $\forall a \in A$. Avem : $1 + x = (1 + x)^6 = \sum_{k=0}^{6} C_6^k x^k = x + x^4 + x^2 + 1$, de unde $x^4 = -x^2 = x^2$. În fine, $x = x^6 = x^4 \cdot x^2 = x^2 \cdot x^2 = x^4 = x^2$.

50. Avem $f(1) = 1$, $f(2) = f(1 + 1) = f(1) + f(1) = 1 + 1 = 2$, $f(-2) = -f(2) = -2$, în general, $f(n) = n$, $\forall\ n \in \mathbf{Z}$. Dacă $r \in \mathbf{Q}$, atunci $r = mn^{-1}$, cu m, $n \in \mathbf{Z}$, de unde $f(r) = (fmn^{-1}) = f(m)f(n^{-1}) = f(m)(f(n))^{-1} = mn^{-1} = r$. Fie g un automorfism al lui $\mathbf{Q}(\sqrt{2})$. Evident $g(r) = r$, $\forall\ r \in \mathbf{Q}$. Dacă $x = a + b\sqrt{2}$, cu a, $b \in \mathbf{Q}$, atunci $g(x) = g(a) + g(b)g(\sqrt{2}) = a + bg(\sqrt{2})$. Dar $2 = g(2) = g(\sqrt{2}\cdot\sqrt{2}) = g(\sqrt{2})g(\sqrt{2}) = (g(\sqrt{2}))^2$; deducem că $g(\sqrt{2}) = \pm\sqrt{2}$. Dacă $g(\sqrt{2}) = \sqrt{2}$, atunci g este automorfismul identic, iar dacă $g(\sqrt{2}) = -\sqrt{2}$, atunci g este automorfismul cu acțiune $a + b\sqrt{2} \to a - b\sqrt{2}$.

51. Se observă că $f(r) = r$, $\forall\ r \in \mathbf{Q}$ (v. Ex. 50). Dacă $x \in \mathbf{R}$, $x > 0$, atunci $f(x) > 0$. În adevăr, fie $y \in \mathbf{R}$, $y > 0$ astfel încît $y^2 = x$. Atunci $f(x) = f(y^2) = (f(y))^2 > 0$.

Fie $x \in \mathbf{R}$, $\varepsilon > 0$ și r_1, $r_2 \in \mathbf{Q}$, $x - \varepsilon < r_1 < x < r_2 < x + \varepsilon$. Atunci $f(x - \varepsilon) < f(r_1) < f(x) < f(r_2) < f(x + \varepsilon)$, deci $r_1 < f(x) < r_2$, de unde $|f(x) - x| < \varepsilon$. Rezultă că $f(x) = x$, $\forall\ c \in \mathbf{R}$.

CAPITOLUL V

3. Avem $f_*(g_*x) = f_*(g(x)) = f(g(x)) = (f\circ g)(x) = (f\circ g)_*x$; $1_M{}_*x = 1_M(x) = x$.

6. K^n are 2^n vectori.

7. K^n, unde $K = \mathbf{Z}_p$.

8. Fie $v \in V$, $v \neq 0$. Atunci aplicația $\mathbf{R} \to V$, $\alpha \to \alpha v$ este injectivă.

9. $x + x + \ldots + x = \hat{1}x + \hat{1}x + \ldots + \hat{1}x = (\hat{1} + \hat{1} + \ldots + \hat{1})x = \widehat{p}x = \widehat{0}x = 0$.

11. $v = (-3)v_1 + 0\cdot v_2 + 5v_3$.

12. $A = -5E_1 - E_2 + 6E_3 - 2E_4$.

13. $f = 3f_1 - 9f_2 + 5f_3$.

14. $f = 1 + (-1)X + (-1)X^2 + X^3 = 1\cdot(1 + X^2) + (-1)(X + X^2) + (-2)X^2 + 1\cdot(X^3 + X^2) = 0\cdot 1 + 0(X - 1)/1! + 4(X - 1)^2/2! + 6(X - 1)^3/3!$.

CUPRINS

